SPARTA

# D1.4

# Lessons learned from externally assessing a CCN pilot

| | |
|---|---|
| **Project number** | 830892 |
| **Project acronym** | SPARTA |
| **Project title** | Strategic programs for advanced research and technology in Europe |
| **Start date of the project** | 1st February, 2019 |
| **Duration** | 36 months |
| **Programme** | H2020-SU-ICT-2018-2020 |

| | |
|---|---|
| **Deliverable type** | Report |
| **Deliverable reference number** | SU-ICT-03-830892 / D1.4 / V1.0 |
| **Work package contributing to the deliverable** | WP1 |
| **Due date** | April 2021 – M27 |
| **Actual submission date** | 9th June, 2021 |

| | |
|---|---|
| **Responsible organisation** | Fraunhofer |
| **Editor** | Dirk Kuhlmann |
| **Dissemination level** | PU |
| **Revision** | V1.0 |

| | |
|---|---|
| **Abstract** | This document assesses the structures, processes and activities characterizing the governance of the SPARTA pilot during its second year. Assuming an external perspective, the governance elements are analysed in view of their adequacy for a future network of national Cybersecurity Competence Centres (NCCNs), European Cybersecurity Competence Centre (ECCC). The study discusses options for adapting SPARTA's governance related activities in view of the remaining period. |
| **Keywords** | Governance, pilot, structure, process, Cybersecurity Competence Network, Cybersecurity Competence Centre, CCN, ECCC, NCC, assessment, external |

This project has received funding from the European Union's Horizon 2020 research and innovation programme under grant agreement No 830892.

**Editor**

Dirk Kuhlmann (Fraunhofer)

**Contributors** (ordered according to beneficiary numbers)

Florent Kirchner, Augustin Lemesle, Thibaud Antignac (CEA)

Dirk Kuhlmann, Michael Friedewald (Fraunhofer)

**Reviewers** (ordered according to beneficiary numbers)

Christian Derler (JR)

Andrius Bambalas (MRU)

## Disclaimer

# Executive Summary

SPARTA is one of four pilot initiatives investigating operative aspects of a future European Competence Centre and Network for Cybersecurity (ECCC/ECCN). As of April 2021, the role, structure, and function of this institution has been agreed upon by the EU member states, while its topical scope is still in flux. SPARTA's governance model can now be evaluated against a fixed target.

The main governance objective is to safeguard efficient project management using a structure of boards and work packages for all main activities. A second objective is to track the progressive implementation of the ECCC and to adjust activities accordingly towards more coordinated efforts of all four initiatives. With the exception of the Advisory Committee, all of SPARTA's task forces are active and contribute to collaborative, inter-pilot focus groups.

This report assesses SPARTA's governance during its second phase of work, i.e., from February 2020 to January 2021. Its two parts comprise a multi-perspective analysis by consortium member Fraunhofer ISI (PART 1) and an independent study commissioned from the external contractor Technopolis (PART 2).

The general view of the Technopolis study is positive. Room for improvement exists regarding the horizontal and vertical interactions in the project, clear distinction between activities of the Executive and the Strategic Board, feedback and influencing opportunities for the group of associates and friends, inter-pilot collaboration. It also observes a lack of opportunities to put SPARTA's governance concepts to a real world.

According to the ISI analysis, SPARTA anticipated the governance implications of the political row towing about the ECCC quite well. This is confirmed, in retrospect, by the similarities in the respective governance structures and their topical foci. Substantial differences between pilot and institution exist regarding the constituencies of the boards, the powers of the Executive Director, and the decisive role of national cyber competence centres (NCCCs), e.g. for the admission of associated community members. Central aspects of the future ECCC governance could not be modelled in a pilot scenario, so transferability of experiences with specific aspects of governance is often limited, or does not exist, as in the case of NCCCs.

**Results**

The external study sees room for improvement regarding the horizontal and vertical interaction between work packages and governance, for a clearer definition of executive and strategic governance roles, opportunities of including SPARTA's friends and associates, and for collaborative activities with the other pilots.

The lessons learned during this work period suggest paying attention to three specific aspects in particular. Members of the SPARTA Associates program should be encouraged to move towards a European cybersecurity community. Parallel international activities like the OpenSSF and the OCA will have to be accounted for. Technical and non-technical activities should be re-evaluated and transitioned to the ECCC, into follow-up activities, or into inter-pilot activities.

# Table of Contents

# PART 1
# Internal multi-perspective view

This page is intentionally kept blank.

# Table of Content

# List of Tables

# Chapter 1 Introduction

This document is the second of three studies on the governance of the SPARTA CCN pilot for the planned European Cyber Competence Centre (ECCC) and Cyber Competence Network (ECCN). The first assessment covered the work period until early 2020. It primarily assumed a pilot-internal perspective and assessed itself using methods that were specifically developed for this purpose. In contrast this study analyses SPARTA's governance in 2020 and early 2021 and is carried out assuming external perspectives. This happens in two ways. Firstly, this deliverable includes an assessment from an external evaluator who is completely independent of the project consortium. Secondly, the complementary analysis carried out by consortium member Fraunhofer ISI is now less concerned with internally defined metrics and KPIs corresponding to the Call for Proposals (CfP), and more with the relevance and applicability of SPARTA's governance to the future, real world institutions.

This change of vantage point reflects the substantial progress towards the actual implementation of the ECCC an ECCN that has been made in the meantime. The final draft for the *Regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres* was agreed upon by the member states in December 2020. As of April 2021, the legal terminology of this draft is under review, and translation into the various languages of the EU member states is underway. The final text should be ready for ratification in the second quarter of 2021.

In February 2021, Bucharest was chosen as the geographical location for the ECCC[1]. The member states have since been asked to nominate the respective institutions acting as National Competence Centres. In mid-April 2021, the future Governance Board members had their first informal (and virtual) meeting[2]. In parallel, the European Commission (EC) has asked the four pilots for their suggestions on the main strategic directions that should be pursued during the initial phases of the Centre.

Hence, multiple intermediate milestones have now been reached, and the governance activities of all Cyber Competence Network (CCN) pilots, have to account for this. Until recently, the main task of the pilots to explore the range of *potential* future activities of a European Cyber Competence Centre to the widest extent possible. As the political compromise between the EC and the EU member states about the *actual* range of the centre has now been reached, the pilots have to take stock of their achievements so far. Activities with a fair prospect of being transferred to the future institution ought to be distinguished from those whose chances are reduced, and options for re-allocation of resources may have to be considered.

Attention should also be given to future concerns of the institutionalized ECCC that may go beyond the current brief of the pilots, as it turns out that not all angles could be covered within the perimeters of the call for proposals from 2019. Such constraints are also caused by the procedural rules applicable for EU funded research projects, or by unpredictable changes of context, and due to uncertainties of the results of political negotiations. Notably, this concerns the interaction between Cyber Competence Centres (CCCs) at national and European level, the governance board dynamics caused by specific national interests, level of contribution, and internal competition for research and infrastructure funding.

The final version of the ECCC Proposal for Regulation now defines the exact scope of the European and national responsibilities. The implications of the resulting power balance would warrant a closer look. Unfortunately, the implications cannot easily be tested in the context of a CCN pilot. In particular, this concerns the effect of financial incentives on furthering strategic European goals, or the modality of involving desirable technology partners outside the European Union in projects with

[1] https://www.politico.eu/article/5-reasons-why-bucharest-won-the-eu-cyber-competence-center-race/
[2] https://digital-strategy.ec.europa.eu/en/news/european-cybersecurity-competence-centre-and-network-moves-forward-future-governing-board-meets

stringent secrecy requirements. The dynamics created by national CCCs entitled to act as gatekeepers for access to a cyber-competence "community" is equally hard to test. These factors, although being essential for the future operation of the centre and the network, cannot realistically be simulated, even in experimental environments like those of the CCN pilots.

This study differs from its predecessor D1.2 in both approach and outlook. In the interest of obtaining a fresh and unbiased view, the bulk of the assessment was assigned to an external entity. The new external study complements the methodology of D1.2 from 2020, which had mainly targeted internal causes and effects. In contrast, this deliverable focuses on the environment and external interfaces of the pilot (and, in extension, on those of the future European and National CCCs), and it re-frames pilot governance activities in the wider context of European and national institutions.

Including a full external assessment is more than just due diligence. The original Draft Proposal from 2018 and final draft regulation adopted in 2021 foresee external evaluations. They are instruments of the ECCC Executive Director's toolbox for safeguarding continuous monitoring and evaluation. Consequently, the external assessment of SPARTA was also carried out in view of partial re-usability in a future, real-world scenario. This regards the criteria and methods applied by the commissioned, external study in PART 2, however, the procedural aspects of preparing and carrying out the assessment are of possible interest as well. Lessons can and have been learned at every step of the process -- formulating a sound invitation for tender, making decisions on initial scoping and access to internal documents, fine-tuning the scope with the external assessors, and supporting them during the fact-finding period. Some tasks turned out to be more complex than expected. In combination, the methods of D1.2 and D1.4 provide a lightweight approach assessing a CCC-type organization, and we hope that they may support future executives of the ECCC in their tasks.

The pre-final ECCC Draft Proposal for Regulation dates from December 16, 2020. The document was not yet at our disposal when publishing the call for tender for the external assessment, nor when and fine-tuning the scoping with the successful bidder. Since the dissemination of the Draft Proposal is restricted, it could not be shared with the contractor at a later stage. The task of matching observations of the commissioned, external study with the Draft Proposal is therefore covered by Fraunhofer ISI who, as contributing editor, had access to this draft. This also applies for the analysis of contextual changes for cybersecurity during the work period. This aspect was scoped out from the external study, as its treatment would have required a degree of familiarity with the subject matter that could not be expected from the assessor.

One noteworthy contextual change regards the creation of two international bodies dedicated to issues of Open (Source) Software security in 2019/2020. These two initiatives, the Open Cybersecurity and Open Source Software Security initiatives (OCA resp. OpenSSF) are geared towards global community of stakeholders and contributors. Their outreach strategies differ from and compete with those envisaged for the future ECCN OCA (European members only). Some implications will be discussed in this study.

The aim of "externally" assessing the SPARTA pilot raises the question on the most appropriate vantage point(s) for the investigation. In the interest of objectivity, the external assessors (PART 2).have taken a high-level view for analysing the institutional context and used empirical approach for determining details on specific details. In contrast, the analysis from Fraunhofer ISI (PART 1) takes a multi-perspective view. This allows to reflect the position different stakeholders, such as the EC, the SPARTA associates (as prospective members of national cyber competence networks and communities), and the cybersecurity research community. These perspectives and findings are translated into a list of generalized observations and lessons learned.

**How to read this document**

This report consists of two main parts. Editorial considerations suggested placing the assessment of the external contractor into the second position. This resulted in various forward references in those sections of the first part that discuss results from the externally commissioned study. Readers are therefore encouraged to familiarize themselves with the results of the external assessment in PART 2 before reading PART 1.

# Chapter 2 A multi-perspective view on SPARTA

## 2.1 The past and future function of CCC / CCN pilots

In this section, we briefly recapitulate the history leading up to the implementation of the CCC pilots and contextualize the current state-of-affairs. Additional details can be found in D1.2 and in PART 2 of this study.

In late 2017, the perceived increase and severity of cyber-related attacks, including those of supposedly government-sponsored adversaries, let the EC spring into action. After some months of preparation, a political announcement of a future European Cybersecurity Competence Centre was made in 2018. It was accompanied by a draft regulation for such an institution.

In order to determine the scope of this institution, to gain some first insights on how to run it, and to acquaint the cyber-security community with the idea of a new European body, a CfP was issued. It invited proposals for piloting and exploring the future competence centre and network. Four consortia were successful in their bids, SPARTA being one of them.

The projects took up this work in early 2019. Since then, further details of the future institution have been refined in political negotiations between the EC and the member states. It required a drawn-out process, but a final agreement finally reached in December 2020. As of April 2021, this draft Proposal is under legal review, and translation into the languages of the member states is on the way. The final Proposal for Regulation is expected to be ready for ratification within a few months.

While the negotiations went on, the main task of the CCC pilots was to explore alternatives for strategic focus areas and the organizational and procedural aspects of governing the future ECCC and network. The precise results of the political negotiations were unknown during this period. Consequently, a wide range of conceivable outcomes had to be addressed. This was enabled by the different profiles of the four pilots. For covering a multitude of angles, they were initially encouraged to pursue their goals independently and competitively. Intermediate results of all pilots were presented at regular consultation meetings, thereby supporting the EC in path planning for different conceivable outcomes of the political negotiations.

As these negotiations converged, the necessity for inter-pilot co-ordination became more prevalent. In particular, this concerned transversal activities common to all projects: dissemination and interaction with the wider community, governance principles, education/training programs and curricula, security certification, and technical road mapping. We are now at the beginning of the phase of the ECCC and by the National Cyber Competence Centres, which are soon (May 2021) to be nominated by the EU member states. The EC has therefore asked the pilots for suggestions for defining the main technical focus areas to be addressed.

The final ECCC/ECCN Proposal for Regulation is an important milestone and potential turning point for some activities pursued by the pilots. Up to this point, their main function was to keep as many options open as possible and to support the EC by exploring a wide range of realistic scenarios. For the remaining period, the function of the pilots will be geared at consolidating results, co-ordinating or merging transversal and research activities common to more than one pilot, and at re-evaluating the relevance of their activities for a future European institution and network operating within the constraints of the Proposal. Only the commission has full overview of the individual contributions from each pilot up to this point, including actual adoption of contributions in the final version of the Draft Proposal and is in a position to make an authoritative "external" judgment on the merits of the contributions for the four pilots.

The purpose of staging four ECCC pilots in parallel was to keep all angles covered for the time of ongoing political negotiations and during the ramping-up phase. Eventually, one option (or some hybrid) has to win out over the others, and the alternatives have to be dropped. We also note that the governance structures and processes of all four pilots have various similarities, so that claims to originality -- may be misguided.

Still, some insight can be gained from comparing SPARTA's governance model with that of the final Draft of the *Proposal for a Regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres*.

The draft version does not yet include an appendix with estimates on staffing and expenditure. Updated estimates have to account for the new financial provisions defined in Article 26 of the final draft version. The exact wording and numbering of the actual regulation might differ from the draft. Differences are expected to be minor and of linguistic nature only and are unlikely to affect the substance of the proposal[3].

The following section summarizes core aspects of the document. In contrast, the external assessment in PART 2 of this document is based on the initial first proposal from 2017/2018.

**Lesson learned:** The main purpose of SPARTA and all other pilots is to present alternatives and to keep options open. The adoption of a piloted concept by the ECCC may count as a measure for its relative success, but does not diminish the merit of discarded alternatives.

## *2.2* Topical Clustering of the *Draft Proposal for a Regulation*

For a contextualized outline of the ECCC, the ECCN and the NCCCs, the reader should consult D1.2 and the introductory sections of the commissioned external assessment in the second part of this document, which also includes a corresponding diagram. Here, we do not aim at a comprehensive overview or alone a detailed legal analysis. Instead, we just cluster regulatory details scattered across the text by topic and summarize a number of regulatory details that are of interest for their commonalities and differences with SPARTA. This allows a point-by-point comparison to the SPARTA governance model.

1. The ECCC and ECCN will be a European Institution in its own right, governed by representatives from each member state and from the EC. Its Governance Board will consist of some 28 participants, 2 EC representatives, plus an ENISA observer without voting right. Decisions have to be endorsed by 75% of the votes. They must also represent at least 75% of the contributions (Art. 15.3). The EC holds 26% of the votes and thereby has a blocking minority for many important decisions, including financial matters, reimbursement, strategic direction and annual work plan.

2. The mission of the ECCC is to give strategic recommendations for research, to implement corresponding actions with EC funding, and to facilitate cooperation between national CCCs and within the competence community. It is noteworthy the ECCC is entitled to fund, acquire and operate ICT infrastructure on its own, if so required by specific tasks (Art. 4.c) -- even in the absence of co-funding by member states.

3. Initially, the ECCC funds will come from the Digital Europe and Horizon Programmes, but other programmes may eventually be tapped if they include aspects of cybersecurity (Comm. 2.3). Intermediate drafts of the Proposal were distributed to multiple (>10) EC institutions, and cooperation between the ECCC and no less than eight European agencies and institutions (Art 10.1) is envisaged. This suggests that within the EC, cybersecurity is perceived as an objective that cuts across institutions and directorates.

4. The ECCC may give advice to an individual member state, but only following an explicit request of this state (Art. 4a.1.5).The ECCC regulation has no prejudice to national competences regarding defence, national security, areas of criminal law, public security and education (Art. 1.4, Art. 12.b), nor does it have prejudice over EC rules on the civilian nature of project funded by the Horizon

[3] Personal information from Martin Übelhör, European Commission, on April 16, 2021

programme. Within these limits, the ECCC aims at enhancing coordination between the cybersecurity civilian and defence spheres (Art 4.a.2).

5. The independently appointed ECCC Executive Director is responsible for implementing the board's decisions, but has no voting rights. In particular, the director approves the list of actions selected for funding based a ranking list established by a panel of independent experts (Art 17.l).

6. The Executive Director is responsible for producing annual reports on the progress towards the ECCC/ECCN mission and objectives (Art 28.d). The regulation defines no criteria or methods for determining the relative level of progress. The Executive Director is also responsible for safeguarding proper monitoring and evaluation of the ECCC (Art 13.3n). Both internal and external auditing is envisaged (Art 17s, Art. 22.8). The governance board is responsible for following up the results of evaluations (Art 17g).

7. The governing board can invite any other person (Art. 14.3); the chairperson of the board may invite representatives of the cybersecurity competence community (Art. 14.4.4). Participation of individuals who are not community members is also possible if they are appointed as advisor or expert by a board member (Art 14.5) -- subject to rules not yet defined.

8. Board and director are supported by a Strategic Advisory Group, which consists of individuals representing entities of the ECCN's cyber competence community. Prospective members of the Advisory Board have to be proposed for appointment to the Governing Board by the Executive Director (Art 13.3.j, Art. 18.1). Membership on the Advisory Board is limited to two years; it can be extended once for the same period.

9. For becoming members of the ECCN, organizations nominated as National CCC must first be endorsed by the EC. The endorsement predicated on a positive assessment of the applicant's capacity and expertise (Art 6.4). NCCCs have to cooperate through the ECCN if relevant to address specific objectives (Art 8.1), e.g. for harmonizing the national CCC entry assessment process. One role of the ECCC is to foster this type of cooperation. For example, guidelines will be produced by the ECCC to support the harmonization of assessment criteria governing membership to the cybersecurity competence community (Art 7aa, Art. 13.3.e).

10. The CCC community consists of national clusters; access is restricted to organizations (i.e., no membership for individuals). The national CCCs act as assessment and registration agency for community members (Art.7h). National CCCs are under the obligation to enable the participation of civil society. However, prospective or current members of CCC communities can be rejected or excluded on the grounds of "justified security reasons" (Art. 8.4). Until harmonized criteria are in place, decisions of this will be based on national considerations and regulation (the provisions made in Art. 8.5 only apply to confidentiality violations affecting the grants agreement process).

11. Interactions with European and international institutions will be carried out within a framework of working arrangements (Art 10.2, Art 13.3). Applicable rules for information sharing are the directives No. 2015/443 and 2015/44; the confidentiality requirements laid down in Art. 330 of the TFEU Treaty apply (Art. 36.4). The regulation also includes provisions for restricting access to licensing, results and background for IP transfer and licensing to third countries (Art.34g). Fort both ECCC and NCCCs, specific rules apply regarding conflicts of interest and access of the public and of interested parties on activities and results (Art 35.2)

## 2.3 Assessment of the SPARTA Governance Model by Topic

**Perspective:** Entities responsible for implementing the future ECCC and the network of NCCCs.

**Note:** The assessment uses a simple 3-point metrics for transferability of governance aspects where "High" corresponds to 3/3, "Partial" to 2/3, "Limited" to 1/3 and "None" to 0/3 points.

We will start out by revisiting some of the non-formal, introductory comments in the Draft Proposal that include general considerations or concrete examples not included in the legal text. The tasks assigned to the envisaged ECCC and the NCCCs are similar to those adopted by SPARTA from the outset or taken up on the way: capacity building, providing expertise, fostering engagement, and enabling coordination (preamble commentary 12). Similarities also exist regarding the stakeholders. Future NCCCs will have to engage: organizations from industry, the research community, the public sector (Art. 7.1.aa, preamble commentary 12a) and civil society (preamble commentary 6).

Civil society aspects are reflected in SPARTA's ELSA[4]-dedicated WP2. However, the activities of WP2 do not currently involve organizations such as consumer associations or trade unions -- to name two examples from the commentary section. SPARTA currently maintains links to the Free and Open Source Software community (preamble commentary 6) through several individual consortium members, but not as an organization, and not as co-ordinated technical or strategic activity. We will revisit this point later.

The strategic planning process envisaged for the ECCC (preamble commentary 15) mirrors the road mapping activities of SPARTA's WP3. The request to all pilots for suggestion on the initial strategic focus of the ECCC (March 2021) issued by the EC is a precursor for similar future requests to the ECCC Strategic Advisory Group.

SPARTA's Strategic Direction Board comprises of the technical director, the work package leaders, individuals tasked with co-ordinating the technical and non-technical work streams in their entirety, and those who continuously monitor the research-political context for relevant changes. This design safeguards a balanced representation of those stakeholders who have responsibilities beyond the contributions of their own organization. Its practical implementation happens to coincide with a balanced distribution of academic and industrial, private and public, large organization and SMEs representation with a good geographical diversity. The level of diversity achieved thereby, however, is a secondary effect, while this has to be a matter of planning for the future ECCC (preamble commentary 27).

We now compare the ECCC governance topics isolated in the previous section with SPARTA's governance structures, processes, and tasks. For each of these topics, we estimate the transferability of experiences from the pilot to a future ECCC governed by those principles that are laid down in the Draft Proposal.

**Point by point Comparison**

1. **Governance Board representation, voting and veto mechanism:** The Draft Proposal rules regard to the distribution of voting rights and blocking minority have no correspondence in the pilot governance model. The observatory role of ENISA in the ECCC Governance Board is mirrored by ENISA's participation in the EC project reviews of SPARTA.

Transferability: None (0/3)

2. **Mission, tasks, scope, Strategic Advisory Group:** The ECCC's mission to give strategic recommendations for research corresponds to the road-mapping activity of SPARTA's WP3, in conjunction with the activities of the Strategic Direction Board. The implementation of corresponding actions with EC funding applies to the SPARTA as a project in its entirety as well as to the selection of its technical work programmes, which were designed according to an initial road-mapping process preceding the project.

A Competence Community does not exist yet as such. Limited experiences with facilitating co-operation within a community of this could be gathered from the group of SPARTA associates (e.g. concerning the constitution of national clusters).

As long as the compromise on the final Draft Proposal had not been reached, the tasks of the national CCCs were not clearly defined. Candidates for the national CCCs have not yet been nominated. Due to these essential unknowns, SPARTA has not undertaken efforts for simulating the interface between ECCC and NCCCs.

[4] ethical, legal, and social analysis

SPARTA has not funded or acquired dedicated ICT infrastructure. However, the project explores the implementation of a common, distributed infrastructure utilizing elements of different consortium members.

Transferability: Partial (2/3)

3. **Funding, involvement of and cooperation with other EC institutions:** The provenance of future funding for the ECCC is of no concern for pilot activity. However, it may incentivize organizations to become members in the CCC community at some point in future. With the exception of ENISA and ECSO, the pilot does not maintain active co-operation with other European agencies and institutions.

Transferability: Limited (1/3)

4. **National precedence for cybersecurity civilian and defence spheres:** The advisory function of SPARTA is limited to giving input in support of the ECCC implementation. While some of its results may be applicable in the cybersecurity defence sphere, there are no specific activities enhance the coordination between civilian and defence cybersecurity. So far, all pilot activities were carried out strictly within the constraints of the Horizon programme. Considerations about the prejudice of national legislation are only relevant for SPARTA's initiatives on education and training.

Transferability: Limited (1/3)

5. **Appointment and approval rights of the Executive Director:** In contrast to the ECCC Executive Director, the technical and operational leads of the SPARTA pilot have been nominated from the range of consortium members. Directors have full voting rights. Similarly, in SPARTA, the ranking and selection of actions does not rely on the opinion of independent experts.

Transferability: None (0/3)

6. **Responsibilities of the Executive Director, monitoring and evaluation:** The duties of the ECCC Executive director combine many of the tasks carried out by the SPARTA technical directors: executing decisions taken by the governance board, reporting on progress of implementation in regular intervals, and annual reporting the progress made towards achieving the general mission and objectives. SPARTA's governance has defined procedures for monitoring, internal and external evaluations and has developed corresponding methods, criteria and metrics, including those for assessing the continued relevance of KPIs. In both models, responsibility for following up evaluation results is assigned to the Governance Board.

Transferability: High (3/3)

7. **External participants in Board meetings:** Other persons can be invited to SPARTA Executive Board meetings if agreed upon by the board members. Regarding consortium members, this is in fact standard practice. In the interest of continuous internal assessment, the lead of the responsible sub-WP 1.3 participates in both Executive and Strategic board meetings without voting rights, but with the right to contribute to agenda and discussion. Invitation of outside individuals is possible if the board members agree. For SPARTA's Executive Board, such a situation has not yet arisen. SPARTA's Strategic Direction board has invited the authors of the external assessment study to present the results in one of their meetings. An invitation of representatives from its associate program or external advisors would be possible.

Transferability: Partial (2/3)

8. **Nomination for and appointment to the Strategic Board:** The Draft Proposal and the SPARTA governance model both clearly distinguish executive and strategic activities. In both instances, we find a dedicated board tasked with strategic aspects. SPARTA's board consists of WP and activity leaders who have practical responsibilities for the operation of the pilot. Since the contributors to a particular WP acknowledge their respective WP leaders, board membership implicitly carries some democratic legitimacy: the duration of board membership is not predicated on appointment by a superordinate instance, but on a specific function.

Input for strategic activity is primarily gathered by tapping the expertise and professional connections of the consortium members. Additional input could be sourced from SPARTA's associates and the Board of Advisors, if so required. In practice, the pilot has mostly relied on its internal resources, that is, project partners and board members, not least since SPARTA's associates are not contractually bound to support SPARTA's strategic activities.

The operational activities of SPARTA's strategic activities strongly resemble the tasks that will have to be addressed by the ECCCs Strategic Advisory Group. On the other hand, there are marked differences between the pilot and the future ECCC regarding the constitution of the Strategic Advisory board.

Transferability of operational aspects: High (3/3)
Transferability of structural aspects: Limited (1/3)

9. **Endorsement of and cooperation between NCCCs:** As of April 2021, NCCC candidates have yet to be nominated, and the range of their tasks and responsibilities has only recently been defined. SPARTA has so far not endeavoured to model the interaction between ECCC and NCCCs.

The closest analogy to the constitution of NCCCs and their national competence communities is provided through national clusters (France, Italy, Spain) of the project consortium members and corresponding clusters among the SPARTA associates. Several consortium members, notably from smaller countries like Lithuania, the Czech Republic, Belgium and Luxemburg are candidates for becoming an NCCC or maintain closes links with the nominated institutions.

Although SPARTA's consortium members were selected based on their capacity and expertise, the pilot has not implemented a formal endorsement procedure for entities. Work streams are task-oriented without particular attention given to the nationality of the contributing organizations. SPARTA can currently provide little expertise on facilitating the cooperation between nationally aligned clusters or on harmonizing the assessment criteria for national CCCs.

Transferability: Limited (1/3)

10. **Prerequisites for becoming a member of the competence community:** The SPARTA consortium consists of the organizations that signed the grant agreement. Its associates program primarily targets organizations, but would not categorically exclude membership of individuals. Applicants are acknowledged as SPARTA associate by the lead of the corresponding program. SPARTA model has three tiers of associates; allocation to either of the tiers is based on candidates declaring their desired level of involvement. The pilot does not command the instruments for thoroughly assessing whether an applicant for the associates program should be allocated to a specific tier or rejected for reasons of security.

Transferability: Limited (1/3)

11. **Interaction with other institutions, access to information and IP:** SPARTA's interactions with European institutions happen within the contractual framework of the consortium and the grant agreements, which subjects all of its activities to the applicable EC rules on conflict of interest, data protection, information sharing, confidentiality, and transfer of intellectual property.

The pilot does not address scenarios demanding restrictions of access for some parties. SPARTA aims at the widespread and unconstrained dissemination of its results; all of its deliverables are publicly accessible.

Transferability: Limited (1/3)

**Transferability of SPARTA governance**

| Nr. | Topic | Sections in Draft Proposal | Transferability (range: 0-3) |
|---|---|---|---|
| 1 | Governance Board representation, voting and veto mechanism | Art 15 | n/a (0/3) |
| 2 | Mission, tasks, scope, Strategic Advisory Group | Art 4, Comm. 12 | Partial (2/3) |
| 3 | Funding, involvement of and cooperation with other EC institutions | Art 10, Comm 2.3 | Limited (1/3) |
| 4 | National precedence, coordination of cybersecurity civilian and defence spheres | Art. 4a.1.5, Art. 4.a.2, Art. 1.4, Art. 12.b | Limited (1/3) |
| 5 | Appointment and approval rights of the Executive Director | Art 17 | n/a (0/3) |
| 6 | Responsibilities of the Executive Director, monitoring and evaluation | Art 28.d., Art 13.3n Art 17s, Art 17g, Art. 22.8 | High (3/3) |
| 7 | External participants in Board meetings | Art. 14.3; Art. 14.4.4, Art 14.5 | Partial (2/3) |
| 8,1 | Nomination for appointment to the Strategic Board (procedural aspects) | Art 13.3.j, Art. 18.1. | High (3/3) |
| 8.2 | Nomination for appointment to the Strategic Board (structural aspects) | Art 13.3.j, Art. 18.1. | Limited (1/3) |
| 9 | Endorsement of and cooperation between NCCCs | Art 6.4 Art 8.1, Art 7aa, Art. 13.3.e. | Limited (1/3) |
| 10 | Prerequisites for becoming a member of a national competence community | Art.7h Art. 8.4, (Art. 8.5). | Limited (1/3) |
| 11 | Interaction with other institutions, access to information and IPR | Art 10.2, Art 13.3, Art.34.g, Art 35.2 | Limited (1/3) |

Table 1: Estimates for transferability of SPARTA governance characteristics by topic

In summary, good or partial transferability can be expected for 4 out of 11 governance topics, limited transferability is likely for 5 areas. Two other cases have no equivalent within SPARTA's governance activities.

**Lesson learned:** The transferability of governance mechanisms and experiences varies widely. This indicates that important operational aspects of the ECCC, the ECCN and the NCCCs could not be mirrored by corresponding requirements in the Call for Proposals.

## 2.4 Applicability of ECCC Result Indicators for SPARTA's Governance

**Perspective:** Entities responsible for implementing the future ECCC and the network of NCCCs.

As we are moving towards an institutionalized ECCC, we may ask whether the KPIs envisaged for this institution could be applied to SPARTA's governance (or correspondent to KPIs defined by the pilot). The final list of indicators has not yet been published; however, we may assume that they will be largely similar to those spelled out in the initial proposal from 2018.

Seven tentative result indicators for the ECCC have been defined so far:

1. *Contribution to next cybersecurity technologies, measured in terms of copyright, patents, scientific publications and commercial products*:
   **Applicable**. SPARTA employs similar metrics.
2. *Number of cybersecurity skills curricula assessed and aligned, number of cybersecurity professional certification programmes assessed.*
   **Partially applicable**. SPARTA has produced cybersecurity skills curricula. These, however, have yet to be assessed.
3. *Number of scientists, students, users (industrial and public administrations) trained.*
   **Partially applicable.** Related to point 2, the curricula have yet to be assessed. A provisional comparable metric would be the number of scientists, students and users who entered cybersecurity by joining SPARTA and are thereby "trained on the job".
4. *Number of cybersecurity infrastructure/tools jointly procured.*
   **Not applicable**. No cybersecurity infrastructure or tools are procured by SPARTA, either individually or jointly with other pilots.
5. *Access to testing and experimentation time made possible for European researchers and industry across the Network and within the Centre. Whenever the facilities already exist, increased number of hours available for those communities in comparison to the hours currently available.*
   **Partially applicable.** SPARTA is working on a distributed infrastructure in support of its technical goals that may eventually made accessible to selected partners and associates. -- The metrics suggested in the draft proposal ("time", "hours", "communities") would need to be specified e.g. in terms of time of access to infrastructure, bulk computing cycles per hour, scale-out / parallelization equivalents. Communities would need to be specified in terms of membership criteria (e.g. R&D, industry, SMEs, civic society organizations).
6. *The number of user communities served and number of researchers getting access to the European cybersecurity facilities increases when compared to the number of those having to look for such resources outside Europe.*
   **Not applicable.** SPARTA does not track whether consortium members or associates utilize cybersecurity facilities and resources outside Europe. Establishing a baseline of such utilization at the scale of European research and industry would require a dedicated study. As for "communities", see comment on point 5.
7. *Competitiveness of European suppliers starts increasing, measured in terms of global market share (target 25% market share by 2027), and in terms of share of European R&D results taken up by industry.*
   **Not applicable:** While the dissemination and exploitation of SPARTA results is supported by dedicated activities, this is unlikely to lead to a perceptible increase in the market share of European cybersecurity suppliers. We are not aware of any methodology that would allow to reliably determine causalities between a general increase of market share to the activities of a European research initiative or institution. Should such a method exist, it would have also have to account for the possibility of negative correlation, that is, reduced market share caused by institutional activities.

**Lesson learned:** The result indicators from the first Proposal for a Regulation are mostly unsuitable for measuring aspects of pilot governance, not least because they are loosely defined or questionable on methodical grounds.

## 2.5 Positioning the SPARTA Governance Model

**Analytical perspective:** abstract, scientific view of research exploring governance models.

A high-level indicator for the relative closeness of SPARTA's model to the actual demands of the ECCC and the NCCCs can be obtained by positioning SPARA's within a framework of governance alternatives. A shortlist of alternatives is provided by a recent study from WP3 of the ECHO CCC pilot, which is hereby acknowledged. Based on a theoretical background study and a comparison of some 50 organizations[5], the study has derived four prototypical alternatives[6]. Each of them combines different types of funding, stakeholder communities and their representation, centralization levels, and decision structures, and tailored towards a specific core missions, namely:

- Research and Development
- Education and Training
- Early Warning Systems (Cyber Ranges)
- Innovation and Incubators (Financial Investment)

All four areas need to be covered, in varying degrees, by the ECCC, the NCCCs and the ECCN. Consequently, the ECHO study also presents an "umbrella" model that allows, within limits, to combine aspects of the tailored prototype.

*Where in this framework do we locate SPARTA's governance model?* The pilot governance model is mainly oriented towards the first mentioned prototype, while the order of the bullet list reflects the relative emphasis put on SPARTA's different activities. Its four technical programs are driving R&D on main concerns in current cybersecurity (e.g., the topic of cyber ranges is one of the issues addressed in this context). The technical programs are supported by a dedicated work package (WP3) for continuously updating a technical road map. Education and training is covered by a dedicated work package. It has since produced suggestions for streamlined curricula and educational programs at European scale. The subject matter of incubators and risk capital mobilization comes last on SPARTA's list of priorities, notwithstanding its extensive dissemination and exploitation activities.

*How is SPARTA's model positioned relative to the future ECCC?* We argue that the order of priorities reflected in the bullet list also reflect those of the future ECCC and is therefore identical with those of SPARTA. According to the Draft Proposal, the ECCC's resources for R&D in cybersecurity come from contributions by the member states, the Horizon and Digital Europe programs, and potentially from tapping other European programs. On the other hand, the ECCC will not command operative cyber capabilities and is therefore unlikely to operate an early warning system on its own. Regarding incubators, we note that NCCCs will be appointed by and responsible to the national governments. Hence, the administrative logic of the NCCCs is likely to resemble that of public administration, which is quite different from the administrative logic of agile, innovative environments targeted by private investors.

We conclude that SPARTA and the ECCC correspond to identical prototypic alternatives, namely, the R&D one. This is no coincidence, but a result of a strategic bet. Right from its inception, SPARTA worked on the assumption that NCCCs would retain substantial powers. This assumption was based on the noticeable reluctance of national governments of handing over responsibilities in the security and defence area to European institutions. A second assumption was that the NCCCs would carry the bulk of the overall workload. This was suggested by financial estimates from the initial 2018 Draft Proposal for Regulation, which projects some 80% of overhead costs falling on the national entities.

Many of SPARTA's premises for choosing its governance model correspond to decision criteria that guided the agreement on the final Draft Proposal: as validated in D1.2, SPARTA's governance model addresses every major requirement defined in the Call for Proposals. Why then the limited

**Lesson learned:** SPARTA's governance model as defined in the DoA was chosen in anticipation of a political consensus on the smallest common denominator. This model turns out to be quite close to the one defined in the final draft proposal.

[5] T. Tagarev et al: Governance Needs and Objectives, ECHO Deliverable 3.1, January 2020
[6] G. Penchev et al: Governance Alternatives. ECHO Deliverable 3.2, July 2020

transferability of the governance characteristics and experiences of SPARTA (Table 1)? We would argue that important operational aspects of the ECCC, the ECCN and the NCCCs were simply not reflected in the requirements. E.g., procedures for assigning executive staff, of admitting community members and selecting some of representatives as board members, or considerations on the prejudice of national legislation or stringent access control mirroring a mixture of national and European secrecy requirements simply have no equivalent in the pilot context.

## 2.6 Community Aspects

**Perspective:** Friends and Associates / Cybersecurity Competence Communities

SPARTA is in its third and final work period. It is therefore faced with the challenge of evolving its outreach program towards channelling members of its own associates program into a new, extended ECCC community. Continuous effort will be required to keep SPARTA's associates motivated and the community alive. They will be encouraged to registering with the European Cybersecurity Atlas[7] if they have not done so already.

Some notable differences between the SPARTA program and the European cyber-competence community have already been pointed out. The Draft Proposal installs the NCCCs as gatekeepers assessing candidates for joining their national communities. Mandating an assessment by a national entity as precondition for joining a European community of experts clearly raises the bar, it goes beyond the current informal process of joining the group of SPARTA associates.

The Draft Proposal gives free reign to the ECCC and NCCCs on the specifics of structuring the CC community. While it is clear that working groups will be formed at European level, we do not know how these groups might be mirrored at national level, nor can we be sure whether different levels of community membership will be offered.

For the pilots, their respective group of associates constitutes "social capital" that has so far been closely guarded within the consortia and from other pilots. First insights on this ecosystem are documented in D8.1 and D8.2, and the external study from PART 2 of this deliverable adds some empirical data on the perception of a subset of SPARTA's more than 90 associates. What we are still lacking is a systematic view of the motivations of organizations for joining the associates program of SPARTA (or any other ECCC pilot, for that matter). Strategic considerations, pre-existing links to consortium members or particular individuals, and professional interest are all likely to play a role here, and there may be other reasons as well.

SPARTA is the first of four project facing the issue of community transfer, due to its shorter lifetime (in comparison to the other pilots, who will eventually have to address it as well). An inter-pilot initiative similar to a common brokerage event might be useful for acquainting associates from different pilots with each other. A timely initiative of this kind may be helpful for transitioning the largest possible number of associates into a future ECCC community[8].

**Lesson learned:** It is difficult currently to estimate whether all members of SPARTA's associates and friends program would be willing to join an expanded, inter-pilot group of associates or an ECCC community with a mandatory vetting process.

[7] https://cybersecurity-atlas.ec.europa.eu/

[8] As a side-line, we may be allowed to point out that "community" might not be the most fortunate choice for a designation for the satellite system of institutions, organizations and individuals envisaged by the regulation, since it is just a single instance in a much larger universe of cybersecurity specialists and organizations. The notion of "cyber competence community" can easily be misunderstood, or misconstrued, as a linguistic slide of hand, as a land-grabbing claim of being *the* relevant community representing European competence in cybersecurity. Wherever this kind of attitude is perceived, it risks being called out for grandstanding by a wider community, where membership is primarily predicated on the mutual recognition between peers. ("You cannot call yourself a hacker.

## 2.7 National CCCs

**Perspective**: Entities responsible for implementing the future ECCC and the network of NCCCs.

As EU member states are free in their choice of NCCC candidates. Initial differences between NCCCs are almost unavoidable, due to variations in the type of the nominated organizations, their level of attachment to governmental institutions for defence, security, and criminal prosecution.

Harmonizing the structures and processes of 26 different NCCCs will therefore be at the top of the agenda. The Draft Regulation encourages the cooperation of NCCCs for addressing common problem areas, but makes no provisions on how to support the initial harmonization (in contrast to the admission criteria for joining the CCC community, where guidelines will be issued by the ECCC).

Due to the different political and administrative structures of the member states and their level of autonomy to implement NCCCs, there is not much hope for commonality during the early phases. To address this issue, pilots could offer to "chaperone" the nominated institutions in order to determine similarities between the national approaches. Ideally, this could yield a manageable number of prototypic blueprints that are applicable for more than one NCCC, allowing for co-operation between national institutions whose approaches are roughly similar. Since no single pilot is in the position to cover all of the 26 NCCCs, this issue would have to be addressed as a coordinated, inter-pilot activity. SPARTA might be able to contribute to such an activity with respect to NCCCs from about half a dozen member states. However, any participation in such an effort would first have to be carefully assessed by the EB and SD in view of SPARTA's resources and its remaining lifetime, which may limit the sustainability of this effort.

Regarding the admission to the Cybersecurity Competence Community, NCCCs may hold their own view on the desirability of particular applicants. Certain types of organizations may be encouraged to join, others may be discouraged or find themselves structurally disadvantaged, (e.g. new entrants to the field without records of accomplishment, or organizations from civil society). It might be useful to consider a remediation process at European level, e.g. involving an elected or randomly selected group of community members or a dedicated working group of the strategic advisory board, to address possible complaints of applicants who feel being unduly rejected by their NCCCs.

**Lesson learned:** SPARTA currently provides little, if any guidance for NCCCs. If the projects decides to tackle this issue, it should be addressed as an inter-pilot effort in order to make best use of the proximity of individual consortium members to the NCCCs of particular member states.

## 2.8 Transitioning SPARTA's Results and Activities

**Perspective:** Abstract, analytical

According to the current planning, the SPARTA program will terminate in January 2022. Apart from the individual exploitation plans of the consortium members, there are three major paths for transitioning project results and/or continuing activities: (a) rollout in the context of the future ECCC, (b) supplementary initiatives extending beyond SPARTA's anticipated lifetime, and (c) follow-up R&D projects or supportive actions.

- Concerning path (a), a rollout would be relatively straightforward for the majority SPARTA's transversal activities. We assume that consolidated results of all four pilots would be of interest here. Consolidation efforts for road mapping, education, certification, outreach resp. branding and governance can benefit from the inter-pilot focus groups already in place.
  For a rollout of results from SPARTA's technical programs, different strategies exist. Provided the ECCC's willingness to adopt technical results from the pilots, transfer would depend on the selection strategy adopted: the ECCC could choose a solution from a single pilot, or it could ask for "best of breed" partial solutions from different pilots to be integrated. Similar considerations apply for technical infrastructure, testbeds, and repositories.

- Concerning path (b), the pilots have already been invited by the Commission to extend their activities and to apply for corresponding funding, e.g. for addressing unforeseen gaps or for reacting to changes of context. This option is currently explored by SPARTA's Strategic Direction board, but as of April 2021, no actual decisions have been taken.
- Concerning path (c), the SPARTA consortium is evaluating options to continue some of its activities with selected partners, using the expertise of members of its associates program if appropriate. Planning is in early stages, as it depends on pending decisions about an extension of the project by several months and the publication of suitable calls for proposals from the EC.

SPARTA's transversal activities on ethical legal and social aspects (ELSA) and on certification present specific challenges.

- **Certification**: Certification schemes have been successfully employed for establishing a baseline quality of products and services in many sectors of the economy, ranging from financial services to pharmaceuticals. This observation has given rise to a European political initiative towards mandatory or voluntary IT security certification.

  The cybersecurity community holds no common view on the desirability of EC institutions pushing for mandatory certification schemes. Objections have been raised from all quarters, questioning e.g. the factual merits of current security certification for IT, the technical and economic feasibility and the compatibility with international trade law. The controversy has been amplified by initiatives for advancing software security and safety by lightweight methods, e.g. standardized toolchains and rigorous testing regimes.

  The R&D challenges in this field are so numerous that no single CCC pilot could hope to tackle them alone. If ECCC makes certification one of its strategic priorities, it is this very area where a coordinated, inter-pilot approach and knowledge transfer is most needed. In this context, the question of complementary schemes for Open (Source) Security will have to be addressed as well. This will be discussed in a subsequent chapter.

- **ELSA:** One of SPARTA unique elements is that it addresses ethical, legal and social aspects both at work package and governance level (WP2, Ethics Board). The Draft Proposal, on the other hand, includes no provisions whether and how this area of concern should be reflected in the governance of the ECCC or the ECCC. This also applies at the national level; the member states are free in their choice of an appropriate governance model for their NCCCs. Briefly put, the Draft Proposal encourages contributors from civil society[9] without envisaging formal instruments to make their issues heard (with the exception of contributing to strategic advisory working groups).

  Are there options of translating SPARTA's ELSA activities into operational aspects of the ECCC? Depending on the practical implementation of the ECCC governance, it could be considered to create a dedicated function or advisory committee at the executive level. Such a committed could comprise of members from the Governance and Strategic Boards and with qualified individuals nominated by the CCC community. At CCC level, a strategic working group could be created, whose members may be granted the right to observe and contribute to the work of technical working groups.

  All this would require active participation from organizations and individuals dedicated to adding ELSA perspectives to the technical discourse. Such organizations are not typical candidates targeted by pilot associates programs. They may have to be actively encouraged to apply for these programs and, at a later stage, for CCC membership.

**Lesson learned:** SPARTA needs a staged approach for extending resp. transitioning its results and activities. For most technical and transversal activities with inter-pilot focus groups, there are several alternatives. Special considerations may apply for activities on ELSA and certification.

[9] Final Draft Proposal for Regulation (Dec. 2020), Preamble Commentary 6c, Art 7b, Art 8.2, Art. 18.1,

## 2.9 Open (Source) Security

**Perspective:** abstract, analytical

Open Source Software drives much of the Internet infrastructure, is a vehicle in innovative environments and R&D[10], powers upwards of 2.5 billion end devices[11], and makes inroads into IoT and embedded computing[12]. The importance of this segment for Europe has recently been highlighted in a survey and study commissioned by the EC and co-authored by SPARTA consortium member Fraunhofer-ISI[13]. This study puts the potential annual contribution of Open Source Software to the economy of the EU at around 95 billion Euro.

For this reason, the establishment of two major organizations dedicated to addressing the problem space of cybersecurity by employing open and cooperative strategies. Open Source Software (OSS) security constitutes a major shift not just in the research context for all four CCC pilots, but also for the future ECCC.

The Open Cybersecurity Alliance (OCA) and the Open Source Security Foundation (OpenSSF) cannot be presented in detail here. Briefly put, both organizations are both targeting global audiences. The aim OCA, which is mainly driven by the IT security industry, is to establish standards-based security as an enabler for secure licensing recognized by procurement and policies. This aim clearly overlaps with the ambitions of a European IT security certification scheme. The OpenSSF targets a range of technical topics including as security tooling, securing critical projects, or digital identity attestation. However, it also addresses relating to cyber ranges such as threat identification or establishing security best practices. It should be emphasized that the OpenSSF is backed up by some of the major players in IT[14].

The potential importance of these two initiatives can hardly be overstated, but the implications for the CCC pilots and the ECCC are unclear. We are not aware of any interaction model for European institutions and industry with the OCA and the OpenSSF. It might be necessary to revisit the initial strategic planks chosen for ECCC in view of the work carried out by these organizations. It is not easy to see how the expressly stated ECCC objective of furthering European "digital sovereignty" or "strategic autonomy" can be squared with globally oriented, open initiatives. It is an open question how Common Criteria oriented certification schemes may hold up against a scheme pursued by the OCA. Lastly, it could be a good idea to look for commonalities, interfaces, and complementarities between SPARTA's technical programs and OpenSSF lines of activities.

**Lesson learned:** Due to its limited lifetime, SPARTA can afford not to factor in the international activities of the OpenSSF and the OCA. The ECCC will not be in such a comfortable position. The pilots could support the EC in developing an adequate position and strategy.

[10] https://timreview.ca/sites/default/files/article_PDF/LindmanRajala_TIMReview_January2012.pdf
[11] https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/
https://www.statista.com/statistics/272307/market-share-forecast-for-smartphone-operating-systems/
[12] https://www.w3.org/WoT/IG/wiki/images/9/95/The_essential_guide_to_Open_Source_in_IoT_-_White_Paper.pdf
[13] https://openforumeurope.org/open-source-impact-study/
[14] https://www.msspalert.com/cybersecurity-companies/microsoft-google-ibm-back-open-source-security-foundation/

# Chapter 3 Outlook and Lessons Learned

The external assessment of SPARTA's governance added to our insight by covering a number of aspects not addressed by the initial assessment of D1.2 by providing

- an up-to-date re-contextualization of the pilot's in view of the institutional environment,
- an independent perspective and evaluation of governance structure and processes,
- an analysis of SPARTA's KPIs with a view on their applicability for a real world ECCC,
- feedback from a sub-set of SPARTA's friends and associates,
- suggestions for improving the governance of the pilot.

We note that working with an external party to assess SPARTA's governance required substantial effort, as it involved going through a call for tender at European level. In retrospect, the effort was higher and took more time than expected. In view of possible similar evaluations of an ECCC, we note that the process could be streamlined. Guided by suitable templates, we estimate that the whole process could be carried out within five months under non-pandemic conditions, including the time for tender and contract negotiations.

In financial terms and regarding the additional burden put on the consortium members, the external assessment complied with the demands of a lean and efficient evaluation process demanded by SPARTA's DoA. Overall, we believe that the SPARTA DoA planning correctly anticipated the potential benefits of involving an external party before entering its final work period.

SPARTA's interpretation of the external study (PART 2) is that it gives a generally positive assessment of its governance. The study attests to a number of specific strengths that will not be reiterated here; readers are encouraged to form their own opinion. We confine ourselves to some comments on the potential areas for improvement that were marked out:

- **Limited opportunities and possibilities to act as a real pilot towards the ECCCN:** This result corresponds to the findings from the sections above. It is confirmed by the analysis on the transferability of pilot governance aspects.
- **Internal interaction horizontally (between WPs) and vertically:** This aspect is not covered by the analysis above, as it assumes external perspectives only. However, the result corresponds to several findings from the internal assessment carried out in 2020 in the context of D1.2.
- **Clearer definition of respective roles of the executive and the strategic boards**: At first glance, this is also an internal aspect. However, there is an external angle as well.

  Reflecting executive and strategic concerns in the governance structure -- rather than making it a purely procedural matter for a single board -- has proven to be a sound concept. Actually, it is mirrored in the governance structure defined by the Final Draft proposal. The ECCC's executive and strategic objectives have been assigned to two fully independent boards. However, individuals holding a seat on SPARTA's Executive board also have a seat on its Strategic board, and this is where some of the confusion on the respective roles of both boards may come from.

  We also observe that situations of urgency sometimes dictate to discuss executive matters in the context of strategic meetings or vice versa, so the separation between both types of concerns is not always maintained. For the real-world ECCC, this confusion should not occur in this form, since the executive and the strategic boards will be staffed by different audiences.

  As far as the deliberations of the Strategic board have implications for the extended group of consortium partners, they will always be communicated by the executive board as one of its decision. Due to this absence of direct interactions with the SD, this board might be considered redundant by those consortium members who do not assume governance roles.
- **Limited possibilities of associates and friends to influence SPARTA activities**: This describes the status quo ante quite accurately. However, SPARTA's options of taking up

influences of this type are rather limited. As an EU funded project, it is under contractual obligation to deliver the results promised in its DoA. Within these constraints, it also has to adjust to the evolution of its environment with particular regard to the steps taken towards the implementation of the real-world ECCC and ECCN. This state of affairs is expected to improve once the initial strategic focus of the ECCC has been defined, offering incentives and opportunities of contributing to extended activities, follow-up projects or support actions.

- **The challenge/feedback collection form is not optimal for data collection**: This point is acknowledged without further comment; it should be addressed swiftly.
- **Collaboration with the other pilots**: The observations of the external assessment correspond with the results of our analysis made in the previous sections.

### Summary of Lessons Learned

1. **Function of CCC pilots**: The main purpose of SPARTA and all other pilots was and still is to present alternatives and to help keeping options open. The adoption of a piloted concept by the ECCC may count as a measure for its relative success, but does not diminish the value of its alternatives.
2. **Transferability of experience:** The transferability of SPARTA's governance mechanisms and experiences varies widely. This indicates that important operational aspects of the ECCC, the ECCN and the NCCCs could not be mirrored by corresponding requirements in the Call for Proposals.
3. **Applicability of result ECCC result indicators**: The result indicators from the first Proposal for a Regulation are mostly unsuitable for measuring aspects of pilot governance, not least because they are loosely defined.
4. **Positioning the SPARTA pilot:** SPARTA's governance model as defined in the DoA was chosen in anticipation of a political consensus on the smallest common denominator. This model turns out to be quite close to the one defined in the final draft proposal.
5. **Community aspects:** It is currently difficult to estimate whether all members of SPARTA's associates and friends program would be willing to join an expanded, inter-pilot group of associates or an ECCC community with a mandatory vetting process.
6. **Applicability to NCCCs:** SPARTA currently provides little, if any guidance for NCCCs. If the project decides to tackle this issue, it should be addressed as an inter-pilot effort in order to make best use of the proximity of individual consortium members to the NCCCs of particular member states.
7. **Transitioning of results:** SPARTA needs a staged approach for extending and transitioning its results and activities. For most technical and transversal activities with inter-pilot focus groups, there are several alternatives. Special considerations may apply for activities on ELSA and certification.
8. **Open (Source) Security:** Due to its limited lifetime, SPARTA can afford to not factor in the parallel international activities of the OpenSSF and the OCA. The ECCC and ECCN will not be in such a comfortable position. The pilots could support the EC in developing an adequate position and strategy on this matter.

### Conclusions in Summary

The external study sees most room for improvement regarding the horizontal and vertical interaction between work packages and governance, the distinction between executive and strategic governance roles, the influence of SPARTA's friends and associates, and intensified collaborative activities with the other pilots.

The lessons learned during this work period suggest paying attention to three specific aspects in particular. Members of the SPARTA associates program should be encouraged to move towards a European cybersecurity community. Parallel international activities like the OpenSSF and the OCA will have to be accounted for. Technical and non-technical activities should be re-evaluated and transitioned to the ECCC, into follow-up activities, or into inter-pilot activities.

# List of Abbreviations

| Abbreviation | Translation |
|---|---|
| CCC | Cybersecurity Competence Centre |
| CCN | Cybersecurity Competence Network |
| CPPP | Contractual Public Private Partnership |
| DoA | Description of Actions (Project Plan) |
| EB | Executive Board |
| EC | European Commission |
| ECCC | European Cybersecurity Competence Centre |
| ECCN | European Cybersecurity Competence Network |
| ECSO | European Cyber Security Organisation |
| EDA | European Defence Agency |
| ELSA | Ethical, Legal, Social Aspects |
| ENISA | European Network and Information Security Agency |
| EU | European Union |
| KPI | Key Performance Indicator |
| NCCC | National Cybersecurity Competence Centre |
| OCA | Open Cybersecurity Alliance |
| OFE | Open Foundation Europe |
| OpenSSF | Open Source Security Foundation |
| OSS | Open Source Software |
| SB / SD | Strategic Board / Strategic Direction |
| WP | Work Package |

# References

[1] Blind, Knut; Boehm, Mirko; Grzegorzewska, Paula; Katz, Andrew; Muto, Sachiko, Pätsch, Sivan: First Draft on the Second Interim Study Report. Open Forum Europe, Brussels, 2020. (note: refers to an internal draft of the final report)

[2] European Commission: Proposal for a Regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centers. Document 13865/20, revised 16.12.2020. Source: Interinstitutional File 2018/0328 (COD)

[3] European Commission: Establishing and operating a pilot for a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research & Innovation Roadmap. Oct 27, 2017
URL: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/su-ict-03-2018
Checked on 24.04.2021

[4] European Parliament and Commission: Proposal for a Regulation of the European Parliament and of the Council establishing the European Competence Centre and the Network of National Coordination Centres. COM(2018) 630. 12.9.2018. URL:
https://www.europarl.europa.eu/RegData/docs_autres_institutions/commission_europeenne/com/2018/0630/COM_COM(2018)0630_EN.pdf
Checked on 24.04.2021

[5] Kuhlmann, Dirk (Ed.): Lessons learned from internally assessing a CCN pilot. SPARTA Deliverable 1.2.
URL: https://www.sparta.eu/assets/deliverables/SPARTA-D1.2-Lessons-learned-from-internally-assessing-a-CCN-pilot-PU-M12.pd/f
Checked on 24.04.2021

[6] Martinelli, Fabio (ed): Initial results of the clustering, platforms, and ecosystems activities. SPARTA Deliverable 8.1, Jan. 2020
URL: https://www.sparta.eu/assets/deliverables/SPARTA-D8.1-Initial-results-of-the-clustering-platforms-and-ecosystems-activities-PU-M12.pdf
Checked on 24.04.2021

[7] Ordunas, Raul: Intermediate results of the clustering, platforms, and ecosystems activities. SPARTA Deliverable 8.2, March 2020.

[8] Open Cybersecurity Alliance: OCA Charter. Update Dec. 16, 2019.
URL: https://github.com/opencybersecurityalliance/oca-admin/blob/master/CHARTER.md
Checked on 24.04.2021

[9] Open Source Security Foundation: OpenSSF Governance and Legal Documents. Update on Dec. 04, 2020. URL: https://github.com/ossf/foundation
Checked on 24.04.2021

[10] Penchev, Georgi:: Governance Alternatives. ECHO Deliverable 3.2, 2020.
URL: https://echonetwork.eu/wp-content/uploads/2020/11/ECHO_D3.2_Governance_Alternatives_v1.0.pdf
Checked on 24.04.2021

[11] Tagarev, Todor (ed): Governance Needs and Objectives. ECHO Deliverable 3.1, 2020.
URL: https://echonetwork.eu/wp-content/uploads/2020/11/ECHO_D3.1-Governance-Needs-and-Objectives_v1.1.pdf
Checked on 24.04.2021

# List of Partners

| List of Partners | | | |
|---|---|---|---|
| 22 | ANSSI | SECRETARIAT GENERAL DE LA DEFENSE ET DE LA SECURITE NATIONALE | France |
| 7 | BUT | VYSOKE UCENI TECHNICKE V BRNE | Czech Republic |
| 1 | CEA | COMMISSARIAT A L ENERGIE ATOMIQUE ET AUX ENERGIES ALTERNATIVES | France |
| 6 | CESNET | CESNET ZAJMOVE SDRUZENI PRAVNICKYCH OSOB | Czech Republic |
| 4 | CETIC | CENTRE D'EXCELLENCE EN TECHNOLOGIES DE L'INFORMATION ET DE LA COMMUNICATION | Belgium |
| 27 | CINI | CONSORZIO INTERUNIVERSITARIO NAZIONALE PER L'INFORMATICA | Italy |
| 28 | CNIT | CONSORZIO NAZIONALE INTERUNIVERSITARIO PER LE TELECOMUNICAZIONI | Italy |
| 29 | CNR | CONSIGLIO NAZIONALE DELLE RICERCHE | Italy |
| 18 | EUT | FUNDACIO EURECAT | Spain |
| 10 | Fraunhofer | FRAUNHOFER GESELLSCHAFT ZUR FOERDERUNG DER ANGEWANDTEN FORSCHUNG E.V. | Germany |
| 9 | FTS | FORTISS GMBH | Germany |
| 23 | IMT | INSTITUT MINES-TELECOM | France |
| 19 | IND | INDRA SISTEMAS SA | Spain |
| 43 | INOV | INOV INESC INOVACAO - INSTITUTO DE NOVAS TECNOLOGIAS | Portugal |
| 24 | INRIA | INSTITUT NATIONAL DE RECHERCHE EN INFORMATIQUE ET AUTOMATIQUE | France |
| 30 | ISCOM | ISTITUTO SUPERIORE DELLE COMUNICAZIONI E DELLE TECNOLOGIE DELL'INFORMAZIONE | Italy |
| 44 | IST | INSTITUTO SUPERIOR TECNICO | Portugal |
| 40 | ITTI | ITTI SP ZOO | Poland |
| 2 | JR | JOANNEUM RESEARCH FORSCHUNGSGESELLSCHAFT MBH | Austria |
| 16 | KEMEA | KENTRO MELETON ASFALEIAS | Greece |
| 32 | KTU | KAUNO TECHNOLOGIJOS UNIVERSITETAS | Lithuania |
| 33 | L3CE | LIETUVOS KIBERNETINIU NUSIKALTIMU KOMPETENCIJU IR TYRIMU CENTRAS | Lithuania |
| 31 | LEO | LEONARDO - SOCIETA PER AZIONI | Italy |
| 36 | LIST | LUXEMBOURG INSTITUTE OF SCIENCE AND TECHNOLOGY | Luxembourg |
| 34 | LKA | GENEROLO JONO ZEMAICIO LIETUVOS KARO AKADEMIJA | Lithuania |
| 39 | LMT | LATVIJAS MOBILAIS TELEFONS SIA | Latvia |
| 35 | MRU | MYKOLO ROMERIO UNIVERSITETAS | Lithuania |
| 41 | NASK | NAUKOWA I AKADEMICKA SIEC KOMPUTEROWA - PANSTWOWY INSTYTUT BADAWCZY | Poland |
| 17 | NCSR | NATIONAL CENTER FOR SCIENTIFIC RESEARCH "DEMOKRITOS" | Greece |
| 8 | NIC | CZ.NIC ZSPO | Czech Republic |
| 42 | PPBW | STOWARZYSZENIE POLSKA PLATFORMA BEZPIECZENSTWA WEWNETRZNEGO | Poland |
| 11 | SAP | SAP SE | Germany |
| 37 | SMILE | security made in LÃ«tzebuerg (SMILE) g.i.e. | Luxembourg |
| 25 | TCS | THALES SIX GTS FRANCE SAS | France |

| List of Partners | | | |
|---|---|---|---|
| 20 | TEC | FUNDACION TECNALIA RESEARCH & INNOVATION | Spain |
| 3 | TNK | TECHNIKON FORSCHUNGS- UND PLANUNGSGESELLSCHAFT MBH | Austria |
| 12 | TUM | TECHNISCHE UNIVERSITAET MUENCHEN | Germany |
| 13 | UBO | RHEINISCHE FRIEDRICH-WILHELMSUNIVERSITAT BONN | Germany |
| 14 | UKON | UNIVERSITAT KONSTANZ | Germany |
| 5 | UNamur | UNIVERSITE DE NAMUR ASBL | Belgium |
| 38 | UNILU | UNIVERSITE DU LUXEMBOURG | Luxembourg |
| 15 | UTARTU | TARTU ULIKOOL | Estonia |
| 21 | VICOM | FUNDACION CENTRO DE TECNOLOGIAS DE INTERACCION VISUAL Y COMUNICACIONES VICOMTECH | Spain |
| 26 | YWH | YES WE HACK | France |

This page is intentionally kept blank

# PART 2
# External assessment

This page is intentionally kept blank

This part contains the result of external governance assessment made by Techopolis, followed by the call for tender for reference purposes.

This page is intentionally kept blank

technopolis group

*April, 2021*

# Assessment of governance for a European Cybersecurity Competence Network pilot

**Final report**

*April, 2021*

# Assessment of governance for a European Cybersecurity Competence Network pilot

## Final report

Jari Romanainen, Bea Mahieu, Ivette Oomens, Chiel Scholten, Jasper van Dijk, Kincsö Izsak

# Table of Contents

# Tables

# Figures

# Executive Summary

This report provides an independent opinion and support to the SPARTA project's governance by reflecting on its structures, processes and activities. This assignment was implemented in the context of the SPARTA pilot project and also as an experimental template for a future European Cybersecurity Competence Centre Network (ECCCN). The study was conducted between February 15 and April 9, 2021.

## Background

SPARTA is one of the four competence network pilots launched by the Commission to gather experiences for designing and setting up the relevant governance structures, processes, and practices for the future ECCCN. The pilot projects were expected to engage in the following activities:[1]

- "Common research, development and innovation in next generation industrial and civilian cybersecurity technologies (including dual use), applications and services";
- "Strengthening cybersecurity capacities across the EU and closing the cyber skills gap";
- "Supporting certification authorities with testing and validation labs equipped with state-of-the-art technologies and expertise".

The European Cybersecurity Competence Centre Network (ECCCN) has been announced to be set up in 2020 with three components: a European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC), a Network of National Cybersecurity Coordination Centres (NCCCs), and the Cybersecurity Competence Community (the Community). The ECCCN will be "the Union's main instrument to pool investment in cybersecurity research, technology and industrial development and to implement relevant projects and initiatives together with the Network of National Coordination Centres".[2]

The evaluation is based on an evaluation framework assessing the function of the governance structure, principles and processes, programmes and activities in terms of its effectiveness, efficiency, coherence and future relevance. The assessment is based on 25 interviews with internal and external SPARTA stakeholders, a survey and expert-based opinion.

## Assessment against the evaluation criteria

Following the methodology, the main observations of the assessment against the evaluation criteria are presented in the table below:

| **Evaluation criteria/aspect** | **Observations** |
|---|---|
| *Effectiveness* Governance structure | The **governance system and the matrix approach** are viewed as effective in steering and coordinating the project activities, where the route of discussing issues is at the executive board level and then distributing the conclusions to the WPs works well. Leadership is inclusive and open where bottom-up ideas are encouraged. |

[1] EC call for proposals (2017): Establishing and operating a pilot for a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research & Innovation Roadmap. Oct 27, 20178; SU-ICT-03-2018 call for proposal

[2] Final regulation proposal / agreement 2020 "European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres"

| | |
|---|---|
| | The **responsibilities** of WP leaders were not always clearly defined at the start, but it has been clarified over time. The project has tried to ensure a better distribution of responsibilities and shared decision making. Programme leaders have been appointed who are both technical experts and also in charge of the administrative management. |
| | **Strategic Direction meetings and committee meetings** work well. There is consensus about SPARTA's directions. Nevertheless, the executive board meetings are insufficient for the more practical and detailed level communication. The distance between the Executive Board and the Strategic Direction could be improved. Both meetings are run by different people, with the head coordinator of SPARTA only being involved in the Strategic Direction meetings. |
| | **Communication between work packages could be improved.** Attempts have been made to create more linkages it, but the focus has been more on communication tools and software solutions, rather than enough on the underlying governance structure and processes. |
| | The **integration of the transversal WPs and technical WPs** has been refined over time. Nevertheless, since not all partners are involved in transversal WPs, commitment and interaction can be difficult. For technical WPs, the requirements from the transversal WPs can sometimes be felt as a burden upon their daily work. |
| | The **diversity** of people and organisations involved in SPARTA is good, varied, and complementary. Because of this diversity, more time is needed to get to know and better communicate with each other, something that – in particular due to the constraints posed by COVID-19 – could still receive more attention. |
| | SPARTA has a **good balance of various stakeholders** between end users, industry, and research organisations in their network, although the involvement of companies could be strengthened. SPARTA is doing a good job in further expanding the network. |
| | **Decision-making processes are clear** without any micro-management. The delivery teams are empowered and self-organised. Nevertheless, it is important to adopt an even more agile management approach given that the context for SPARTA has been changing fast. |
| *Effectiveness* Governance principles | The **governance principles** have been considered positively in particular the concept of changing risk, diversity and driving the European policy discussion. The governance principle on openness and inclusiveness are adhered to as well. Focus on ELSA aspects is important and something that is special about SPARTA. The adoption of Responsible Research and Innovation and attention for ELSA is important throughout all activities and practices. |
| *Effectiveness* Internal coordination | **Internal coordination** is below expectations. While WP-leaders have sufficient information about other WPs through the Executive Board meetings, this does not ensure sufficient integration of the different WPs. Not all necessary people can be reached effectively. For certain activities such as the development of the roadmap, the absence of face-to-face meetings is a barrier. The **'SPARTA days'** is a governance tool that has been hindered by Covid and is missed the most. |
| | **Work package leaders have been clearly motivated** and incentivised to be active and have been invited to major external conferences where they can have an impact and hence feel the importance of their work. This can enhance |

| | |
|---|---|
| | commitment. Partners feel they can use SPARTA to grow their own network and establish new collaborations, also for new European projects. |
| *Effectiveness* Governance with external stakeholders | **External stakeholders** are less involved in SPARTA as originally foreseen. The COVID-19 pandemic has hindered the organisation of monthly workshops with associates. Partners feel more positive about the role of the Associate Council and the Associates/Brokerage Workshops. Partners are rather positive about aspects related to capturing scientific/educational challenges through interaction with external stakeholders within SPARTA. |
| | **SPARTA is perceived as open and inclusive** towards associates. SPARTA is good at communicating relevant issues on a frequent basis and reaching out for further opinion. |
| *Effectiveness* Governance tools | The **roadmap** is perceived as a good instrument that is responsive to changing needs and trends. Nevertheless, there is no provision in SPARTA to launch projects based on the roadmap and hence it is more of a theoretical exercise and not an instrument for day-to-day steering of the project. SPARTA is not as risk taking and agile as it could be. |
| | The **online SPARTA challenge/feedback** form is not a useful tool, and many are not aware. |
| | **Skills and training activities of SPARTA** are much appreciated. The education map and curricula designer are considered relevant tools. The platform function of SPARTA, for others to access and explore, could be exploited more. |
| | **The SPARTA self-assessment tool was mentioned** as a helpful tool for raising awareness. SPARTA contributions such as the JCCI repository and work with Cyberranges, which enable the exchange and testing of resources and tools. According to some interviewees, it is important to ensure skills and training activities of SPARTA are continued after the project ends. |
| *Efficiency* | SPARTA's governance system has been assessed as being efficient. Internal reporting requirements are necessary and well-organised. The frequency and depth of reporting is adequate. Some are more critical about the value of meetings, for instance related to the time invested in meetings weighing up to the meetings' value in terms of knowledge exchange. |
| | Resources of the SPARTA governance are considered to be sufficient, but extra resources could support better communication between work packages and keeping everyone informed. It has been also pointed out that the European Commission asks for inputs from SPARTA originally not foreseen but these do take resources and attention away from planned tasks. |
| | The monthly meetings of the executive board are reasonable. Nevertheless, the setup of the Executive Board meetings does not always allow for the discussion of important timely issues. |
| | Most of the SPARTA committees convene on an ad-hoc basis, which is considered to be adequate. There are no regular meetings with minutes. Nevertheless, more resources could be spent on publishing meeting summaries to make the project more open and inclusive. |

| | |
|---|---|
| | The large number of partners involved in SPARTA makes it difficult to activate all resources that were originally allocated for their WP, particularly resources planned for cross-WP activities. |
| | SPARTA currently has no budget to experiment with open calls and selecting projects, which makes it difficult to assess the efficiency of the programmes as such. A clear handicap in this respect is that SPARTA is implemented formally as a Horizon 2020 project with administrative framework which is much too rigid to allow the flexibility needed from a pilot action. |
| *Coherence* | SPARTA partners have been generally very positive on aspects related to coherence and SPARTA is considered to be well aligned with the relevant policy needs and priorities. On the other hand, the European Commission could benefit from more direct interaction with and involvement of SPARTA in strategic discussions. |
| | The involvement of SPARTA in ECSO is considered as important and collaboration with ENISA is considered good. |
| | SPARTA is strongly connected with partners across various countries and to the national context. |
| *Relevance* | The SPARTA **governance structure is a governance model that the ECCC can take a lot of inspiration from**. Since the management of research funds is currently not part of SPARTA, its possibilities are limited to act as a proper pilot towards key functionalities planned for the ECCC. SPARTA will be however particularly relevant for managing the community and the interaction between the ECCC and the national centres. |

*Main strengths and areas for improvement of the SPARTA governance*

| **Strengths** | **Potential areas for improvement** |
|---|---|
| Matrix governance structure seems to be the viable approach for SPARTA | Limited opportunities and possibilities to act as a real pilot towards the ECCCN |
| Governance principles and ensuring their implementation in practice: openness and transparency, concept of risk, and diversity | Internal interaction between WPs |
| Proactive approach and inclusion of associates and friends, the tiers-of-trust approach | Internal interaction vertically |
| Roadmap work | The respective roles of the executive and the strategic direction boards |
| The JCCI repository | Interaction with associates and friends |
| Balanced network of relevant actors from research, industry, government, and civil society | Associates and friends feel they have limited possibilities to influence SPARTA activities<br>The challenge/feedback collection form is not optimal for data collection |
| SPARTA activities and the network as a platform for identifying new partners and project ideas | External advisory group |

| | |
|---|---|
| Support for awareness raising, competence development, and training | Collaboration with the other pilots |
| SPARTA governance is efficient | |

## Recommendations

The assessment has identified areas for improvement for SPARTA related to governance bodies, internal communication, outreach, and external communication.

The main **recommendations to SPARTA** are summarised below:

- *Clarify the role of key governance bodies:* There is a need to clarify the roles of the Executive committee and the Strategic Direction committee. The coordinator should consider taking a more active role in the Executive committee.
- *Enhance internal communication:* Further efforts should be made in strengthening communication and interactions between the transversal and technical work packages.
- *Enhance outreach and external communication:* SPARTA should explore ways to further strengthen collaboration with the other 4 pilots to ensure that the relevant experiences and messages are communicated.
- *Ensure learning from SPARTA experiences:* SPARTA should consider working together with the other pilots in preparing a joint policy brief highlighting the relevant experience from all 4 pilots.
- *Continuation to enable real transfer:* SPARTA should consider proposing a limited continuation to SPARTA to ensure dissemination, exploitation, and transfer of SPARTA experience to ECCCN. This could take the form of a Horizon Result Booster project, which is meant for disseminating project results.
- *Strengthen SPARTA as a proper governance pilot and experiment with an adaptive research portfolio*: There have been obvious limitations for SPARTA to act as a proper pilot towards the ECCCN. To overcome the barriers, SPARTA should consider making changes to the work plans of the technical WPs based on changes related to the roadmap and experiment with an adaptive research portfolio. SPARTA could identify synergies between research projects and redirect them for more synergies.
- *Implement a 'fail often, fail fast' approach*: Ideal situation would allow experimentation with the "fail often, fail fast" approach, for instance by launching an open call for new research ideas, selecting several ideas and funding them for a 3 or 6-month initial exploratory stage, and then letting only the most promising one or ones to continue as a full-scale research project.
- *Collecting experiences with managing an unbalanced network*: cybersecurity is an area involving a highly unbalanced landscape of actors as some have more resources and stronger national nodes than others. SPARTA is a good environment to collect relevant experiences from governing such a diverse network and the lessons learnt should be gathered and analysed more systematically.

**Observations related to the ECCCN:**

*Governance principles to be adopted by the ECCCN*

- *Promote openness and transparency*: the ECCC should work in collaboration with stakeholders promoting open access and establishing open platforms, resources, tools, and applications. The primary purpose of this would be to support increased cybersecurity awareness among people and companies (in particular SMEs) in Europe.

The NCCCs could consider a similar approach in a more limited national context, especially if smaller communities of cybersecurity practitioners can be identified who could particularly benefit from mutual exchange of technologies, tools and applications. These communities of practitioners could also extend cross-border in collaborations between NCCCs and possibly also with relevant European institutions.

- *Flexibility and adaptability:* the ECCCN and NCCCN should consider funding modalities which are more acceptable towards risks and changes in the project portfolio. This means not applying the Horizon 2020 type restrictive and highly pre-defined modality of funding projects, but instead more open approaches to selecting, ending, merging, and implementing projects in stages. One possible approach is to launch open calls to select a larger number of projects to test their feasibility and after 6 months or a year, reduce the number of projects by ending, merging, and redirecting some of them to arrive at a portfolio of projects optimally aligned with the roadmap of the call.
- *Promote cross-disciplinary, cross-border, cross-industry, collaborative efforts* : The ECCC, the NCCCs, and the Community should benefit from SPARTA experience in terms of promoting interaction and discussion about controversial and highly important issues, such as openness and transparency, approaches and measures available for developing European strategic autonomy or supply-chain resilience in the global context, or how to increase awareness and reduce cybersecurity risks among European citizens.
- *Balancing act*: The ECCC may have a specific role together with the Commission to define the European way to manage e.g., the balancing act between increasing protection against cybersecurity threats and at the same time protecting access and use of personal data. Developing mobile tracking applications for COVID-19 compliant with the needs and GDPR has been an interesting case. Governance tools

*Governance tools*:

- *Roadmap work:* The SPARTA roadmap offers various lessons for the ECCCN. The alignment of the ECCC roadmap with the one of the NCCCs will require a periodically updating roadmap process to be established in collaboration between the ECCC and the NCCCs. Furthermore, this process will have to include ways to ensure participation of the wider cybersecurity community either directly (collection of views directly from all actors e.g., in the Atlas), or indirectly (collection of aggregated views from the different sub-communities and networks active in the wider European cybersecurity community), or both using a combination of direct and indirect methods. A SPARTA learning point is to put sufficient emphasis on transparency, i.e., publish views or aggregates of them, while clearly indicating for what purposes, how, and when they will be used.
- *Self-assessment and awareness*: The ECCC should together with the NCCCs explore the possibility and viability of adopting, developing, commissioning, or otherwise making available self-assessment tools. This will allow citizens and employees as well as companies, and other organisations to raise cybersecurity awareness and identify and develop targeted trainings for key people and organisations. One of the positive experiences from the SPARTA associates and friends -network is from the use of a self-assessment tool developed in SPARTA for assessing the awareness and knowledge of cybersecurity among an organisation's staff. A possible area for systematic collaborative action between ECCC and the NCCCs could be e.g., implementing awareness and training campaign targeted to organisations and their staff managing critical European and national infrastructures.
- *Audits*: According to SPARTA experience, it is important to remind people of the underlying principles. One possible approach is to use periodical governance audits.

Adoption of principles can be monitored in the context of a wider governance or financial audit, or it can be subject to a dedicated audit.

*Network management and stakeholder interaction:*

- *Tiers of trust*: The approach of establishing networks with partners, associates, friends, outside world has been highly appreciated by the associates and friends. A similar approach could be viable also in the ECCCN landscape. The tiers-of-trust is a viable approach to optimise interactions with the community where there are legitimate reasons to differentiate between external stakeholders.
- *Proactive approach*: The SPARTA experience indicates that proactive interaction is valued by external stakeholders. Rather than relying on making information available, the ECCC and the NCCCs should reserve sufficient resources and establish appropriate processes to enable and encourage proactive interaction with external stakeholders.
- *Brokerage events*: Both the ECCC and the NCCCs can learn from the SPARTA experience with the 'Associates and friends of SPARTA' tool. The main feature of the brokerage events is that they bring together users, companies and researchers around specific user cases and technological opportunities. This has proven a good approach for identifying who else has similar challenges and how potential solutions could be developed. This is also a good basis for identifying partners and ideas for future collaborative projects.
- *Stakeholder engagement*: The ECCCN's future structure should allow for a balanced representation of various stakeholders including both research and industry. In order to allow for more commercialisation of cybersecurity technologies, the governance structure should consider the involvement of industry federations and in particular SME representatives.

*From SPARTA towards the ECCCN:*

- *Setting up a dedicated taskforce*: To ensure that all relevant experiences from all four pilots are transferred as learning points to the design, launch and activities of the ECCCN, a dedicated taskforce to give advice in the remaining planning and launching of the key ECCCN activities is proposed. The taskforce should have members from the four pilots, ECSO, and the ECCC and Commission, and selected representatives from Member states. Such a taskforce can be useful especially in transferring experiences that are difficult to describe explicitly (intangibles). To manage the transfer of experience, the taskforce should continue until all the key activities of the ECCC and the network of NCCCs have been launched.
- *Community support*: The ECCC needs to find a suitable balance between interacting with the network of NCCCs and the wider cybersecurity community and its various sub-communities. The key decision the ECCC and the Commission will have to make in this respect is whether they foresee the need and added value in any action targeted for supporting networking within the wider cybersecurity community at the European level. The support could be based on the tiers-of-trust approach by identifying the most relevant sub-community representatives and giving them a special position. The special position could be in general or it could be more limited to specific actions.
- *Policy alignment*: SPARTA has extensive experience in identifying different policy needs and trends as well as different approaches to cybersecurity related challenges from its roadmap work, collaboration with the other four pilots, work with associates and friends, including national authorities, and more recent work aimed at global actors outside Europe. These experiences may prove valuable especially in view of developing the future activities of the ECCC aimed at capturing potential synergies with other initiatives. The ability of the ECCC and the ECCCN to create added value and impact

beyond the funded projects may depend largely on its ability to capitalise on the potential synergies.

- *Building on the assets of SPARTA*: Important assets of SPARTA to be continued under the ECCCN include the JCCI repository, and the self-assessment tools developed in SPARTA. Another one is the SPARTA 'associates and friends' network.

*Monitoring and evaluation*

- *Measurement*: Monitoring the impact of cybersecurity research and innovation activities is more challenging than in many other sectors. Relevant KPI must be partly based on a realistic counterfactual, which may be an international comparative. One possible counterfactual could be built on risk management, i.e., identifying and assessing the probability and impact of risks related to possible cybersecurity events, and assessing occurred real events and their impacts against the risk assessment. Other possibilities may be changes in numbers of cases over time or estimates of losses cause by breaches. However, making these really viable would also require international comparison.
- *Evaluation system with several layers:* Furthermore, the monitoring and evaluation system will inevitably consist of several layers. The most detailed levels of monitoring are most likely the individual projects and the individual actors. While project monitoring will most likely largely follow existing European and national practices, monitoring of actors will most likely be based on separately organised efforts, such as ad-hoc or periodical surveys. The more aggregated levels of monitoring and evaluation are the initiatives such as collaborative programmes, and the various cybersecurity networks and sub-communities.
- *Establishing an observatory for monitoring:* Monitoring of the initiatives will be largely based on aggregate data collected from projects funded and implemented under the initiative. However, to measure the added value of the initiatives beyond the aggregate of its projects, an additional layer of monitoring must be established. One possibility is e.g., to establishing an observatory for monitoring the developments of e.g., awareness and competences of actors or groups of actors, or monitoring the developments of community networks and sub-communities e.g., through changes in participations and types of engagements over time.

# 1 Introduction

This report is the final deliverable of the 'Assessment of governance for a European Cybersecurity Competence Network pilot'. The evaluation concerns an external assessment as planned in the context of the Horizon 2020 SPARTA project. The study was conducted between February 15 and April 9, 2021.

## 1.1 Objectives of the study

This study aimed at providing an independent opinion and support to the SPARTA project's governance by reflecting on its structures, processes, and activities. This was done both in the context of the current pilot project and as an experimental template for a future European Cybersecurity Competence Centre Network (ECCCN), consisting of the European Cybersecurity Competence Centre (ECCC), the National Cybersecurity Coordination Centres (NCCCs), and the Community.

The assessment focused on the practical efficiency of pilot governance, regarding the internal steering processes and the interactions and interfaces with external stakeholders. It also reflected on the viability of the selected key performance indicators for monitoring the implementation of SPARTA as a governance pilot in the context of the future, real-world scenario.

The assessment evaluated the governance at the Network as well as Programme/Activities level and determined the degree of effectiveness of SPARTA's governance in view of:

- The technical and non-technical goals and objectives stated in the foundational documents (Call for Project Proposal, SPARTA Description of Work)
- The adoption of novel technical and non-technical challenges that may have arisen during the project lifetime.

The evaluation complemented the Yearly Review that is organised in the context of the Horizon2020 monitoring and assessment procedures.

The **evaluation questions** that were formulated for this study are summarised below.

*Table 1 Evaluation questions*

| Area | Evaluation questions |
|---|---|
| Network level governance | • What is the impact of the network governance on the alignment of the results of the Programmes and Activities with the goals of the pilot and objectives of a future ECCCN?<br>• Does the network governance have the capacity to initiate and maintain interactions with variety of relevant stakeholder groups (political administration, national and international agencies, professional bodies, commercial organisations)?<br>• Can they monitor and react to relevant shifts in the research-political and technical landscape of cybersecurity? |
| Programme/Activity level | • What is the achievement of the Programmes in terms of advancing the goals of the pilot as a whole?<br>• Is the interaction of Activities with the Programmes efficient?<br>• Potential and actual impact of the Activities on parts of the external cybersecurity ecosystem<br>• Supportive function of the Activities to the Network- level pilot governance |
| Overall | • What is the feasibility/ practical application of the governance model and its elements being applied in a real-world ECCCN scenario? |

| | |
|---|---|
| | • Which elements of the SPARTA governance practices are applicable in the future?<br>• Is the SPARTA governance model adequate as a blueprint for the ECCC, and what the NCCCs and the Community can learn from the SPARTA experience? |

## 1.2 A note on methodology

The methodological framework used in this study integrates the **theory-based approach** to evaluation which departs from the objectives set for the initiative to map out the 'intervention logic', i.e., the pathway from objectives and activities to outputs, outcomes, and impacts. Evaluation criteria such as relevance, effectiveness, efficiency, and coherence were then used to structure the performance assessment.

These evaluation criteria were used to structure the assessment for the first strand of analysis, directly focused on the SPARTA pilot – as shown in Figure 1, below.

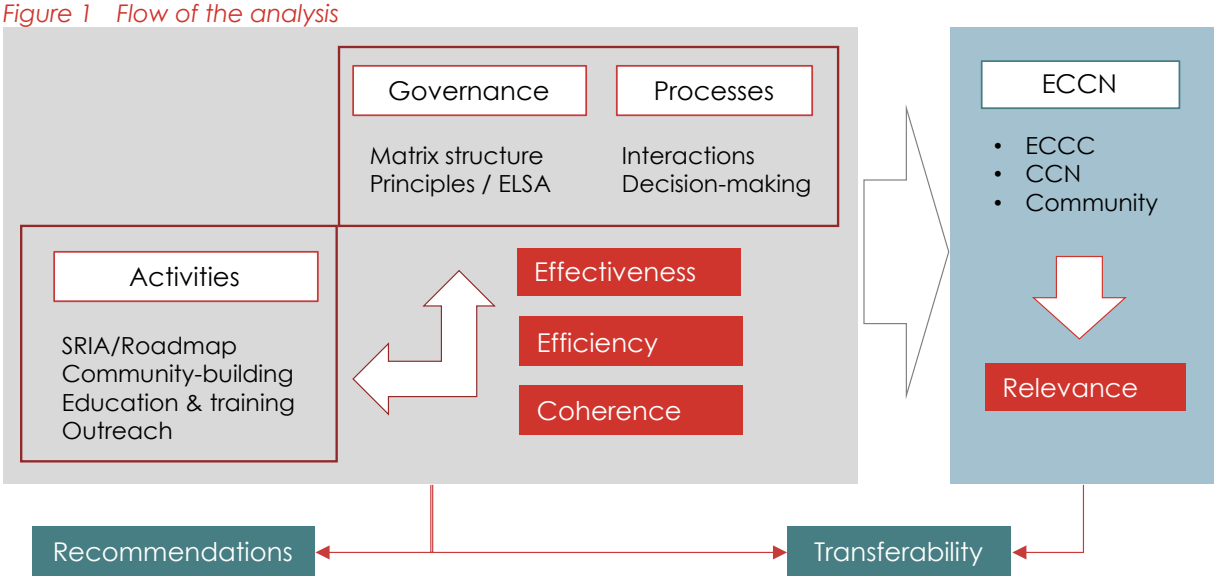
In the context of this evaluation, the evaluation criteria were defined as described below. Central was the function of **governance structure, principles and processes** as drivers and enablers for:

- **Effectiveness** - the functionality of the governance structure, principles and processes in
  - Internally steering and coordinating the activities (the 'vertical' dimension)
  - Enabling interaction and knowledge exchange (the 'horizontal' dimension)
  - Providing interfaces and platforms for interactions with external stakeholders
  - Specific attention will be dedicated to the effects on the SRIA/Roadmap design, the community building activities in WP8 and WP9, and the Dissemination and Communication activities in WP12
- **Efficiency** - the extent to which the governance structure and processes allow for an optimisation of resource utilisation - in particular in relation to the project and programme management
- **Coherence** - the ongoing alignment of the research orientation with the policy needs and other external developments, specifically thanks to the governance structure and processes

A second strand of analysis, running in parallel, focused on the European Cybersecurity Competence Centre Network (ECCCN) and the functions that each of the three components – the ECCC, the NCCCs, and the Community – will be expected to fulfil in the upcoming European cybersecurity governance system.

The extent to which the SPARTA governance structure, principles and processes **could be of relevance** as a model for the implementation of functions and activities in each of these system components was assessed. A **key criterion** for this assessment was the alignment of the SPARTA approach with a) the envisaged structure and processes for the ECCCN components, and b) the principles set out for the Horizon Europe European partnerships.

*Figure 1 Flow of the analysis*




The **outcomes** of the first strand of analysis in combination with the outcomes of the second strand allowed for drawing conclusions on the performance of the governance system in SPARTA and its potential value for the future EU cybersecurity system. It allowed for the formulation of recommendations on adjustments to make in Year 3 of the project to maximise the value of the SPARTA pilot from that perspective.

It equally allowed for the identification of those elements in the SPARTA governance model that merit being transferred and act as a model for the components in the European cybersecurity system.

The data used in this evaluation was collected from relevant documentation, a survey sent to all SPARTA partners (44), associates and friends (90), and in-depth interviews conducted with all SPARTA work package leaders (13) and selected external stakeholders (8). Survey response rates were 77% for the SPARTA partners and 13% for associates and friends. The interviewees represented SPARTA associates and friends (3), similar European initiatives with joint activities or common interests with SPARTA (2), national agencies (1), ECSO board (2).

## 1.3 Structure of this report

The remainder of this report is organised as follows:

- Chapter "Context" provides an overview of the policy context and the key functions and characteristics of the ECCCN and its components.

Chapter "

- SPARTA Governance system" describes the key elements and activities related to the governance structure, processes, and principles of the SPARTA Cybersecurity Competence Network Pilot
- Chapter "Assessment against the evaluation criteria" gives an assessment of the governance of the SPARTA Cybersecurity Competence Network Pilot, against the evaluation criteria (effectiveness, efficiency, coherence, and relevance)

Chapter "

- Conclusions and recommendations" concludes the findings of the assessment of the effectiveness and efficiency of SPARTA's governance, and how it can ensure coherence with policy needs and trends and makes recommendations for supporting the implementation of the final year of SPARTA as a governance pilot, and observations related to translating and adopting of SPARTA experience in the ECCCN landscape.
- More detailed analysis of SPARTA key performance indicators is provided in **Appendix.**

# 2 Context

SPARTA and the three other projects are competence network pilots launched by the Commission to gather experiences valuable for designing and setting up the relevant governance structures, processes, and practices for the future ECCCN. It is therefore important to understand the context in which these pilots and particularly SPARTA have been launched. The following describes why there is a need for coordinated European action in cybersecurity and what steps the Commission has taken and plans to take to establish it.

## 2.1 The need for coordinated European action

The EU initiative of setting up a European Cybersecurity Competence Centre Network is to be set against the context of the need for Europe to step up its capacity to protect Europe against cyber threats and boost the competitiveness of the EU's cybersecurity industry to secure the Digital Single Market.

While there is a wealth of experience and expertise in cybersecurity research, technology and industrial development in Europe, "the efforts of industrial and research communities are fragmented, lacking alignment and a common mission, which hinders competitiveness and the effective protection of networks and information systems"[3]. There is an insufficient level of collaboration between academia and industry, research findings often are not translated into real world solutions, and overall, the European Union still lacks sufficient technological and industrial capacities and capabilities autonomously to secure its economy. In comparison to other global economies, also the investment in cybersecurity capacities and capabilities is suboptimal.

A briefing by the European Parliament on the new European cybersecurity competence centre and network reflects on several key trends within the European cybersecurity landscape. On a more general level, the briefing discusses the societal trend that "critical sectors, such as transport, energy, health, and finance, have become increasingly dependent on digital technologies to run their core business".[4] The growing digital connectivity, fuelled by developments such as increased e-commerce and cashless payments, exposes the economy and society to cyber-threats. At the same time, the **growing number, complexity, and scale of cybersecurity incidents** has an increasing impact on our society and economy. This trend is expected to perpetuate, as it goes hand in hand with technological developments, such as the proliferation of Internet-enabled devices. The briefing discusses that these growing challenges in the cybersecurity landscape have led "the **EU to reflect on how to enhance the protection of its citizens and companies against cyber-threats and attacks"**.[3]

These complexities and threats increasingly undermine the functioning of our communication networks, critical infrastructure, services and ultimately our society itself. Moreover, they have led to increasing concerns among EU citizens, undermining public confidence in the integrity of digital systems and data, and the decisions made using them. According to a survey conducted at the request of the European Commission in 2017[5], **many EU citizens are increasingly concerned about experiencing or being victims of various forms of cybercrime**. For instance, the results show that most respondents worry about things such as: malicious software infecting their devices (69 %), identity theft (69 %) and being a victim of bank card or online banking fraud (66 %)". Furthermore, a recent study conducted by PwC found that the

[3] Final regulation proposal / agreement 2020 "European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres"

[4] European Parliament. (2019). Briefing – The new European cybersecurity competence centre and network

[5] European Commission. (2017). Special Eurobarometer 464a – Europeans' attitudes towards cyber security

number of security incidents has seen a sharp rise across all industries over the past years, with many organisations being inept to adequately respond to cyber-threats.[6]

Moreover, in the light an increasing dependence on non-European cybersecurity providers, actors within Europe increasingly stress the urgency to **achieve technology sovereignty** in this field. To accomplish this, EU stakeholders deem it essential that European cybersecurity research and technological capacities are developed, to secure network and information systems of European citizens and companies, and ensure the protection of critical network and information systems.[7]

These developments stress the urgency to increase EU-wide coordination on various aspects such as knowledge creation, certification, regulation, education and research, and monitoring and advising. The needs have led the main industrial European players to argue for a more coordinated approach, advocating measures that include:[8]

- Addressing (regulatory) fragmentation within the EU landscape by creating a level playing field for enterprises adhering to **"equal requirements concerning data protection and cybersecurity"**, whereas currently it is possible for "non-European players (like Over the Top players / OTT) to opt for the Member State with the least level of protection (e.g., Ireland)".
- EU-wide mechanisms for cybersecurity monitoring and advising that also ensure EU-level harmonization of certification processes, whereas currently the **fragmentation of the European market** is reported to be "the main barrier to the creation of strong European businesses on cybersecurity".
- The **need for skills development and awareness**, not only among individuals but also among European businesses, to be better equipped to cyber-treats.
- **Coordinated research** on 5G - technology and the following generation of mobile standards to "foster cross-sectorial cooperation between CIP-relevant sectors like energy or transport". Cross-sectoral cooperation is reported to be "crucial for the roll-out of, for example, Smart City or Industry 4.0 projects that require a secure, high performance and resilient technology platform".

## 2.2 A partnership

A first action was taken in July 2016 with the launch of the **contractual Public-Private Partnership (cPPP) European Cyber Security Organisation (ECSO)**, as part of the EU cybersecurity strategy. ECSO is a non-for-profit organisation, bringing together "a wide variety of stakeholders such as large companies, SMEs and Start-ups, research centres, universities, end-users, operators, clusters and associations as well as European Member State's local, regional and national administrations".[9] The aim is to "foster cooperation between public and private actors at early stages of the research and innovation process".[10]

Within the H2020 instrument portfolio, a key expected outcome of cPPPs is the common agreed-upon Strategic Research and Innovation Agenda (SRIA), acting as a steering device for the R&I agendas of the research and innovation communities involved as well as providing input to the H2020 Work Programme. Another task of cPPPs is also to foster community building and address specific challenges in the field. In the case of ECSO, specific working groups were

[6] PwC. (2016). The Global State of Information Security Survey 2016

[7] Final regulation proposal / agreement 2020 "European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres"

[8] European Cybersecurity Industry Leaders (n.d.). Recommendations on Cybersecurity for Europe

[9] http://www.ecs-org.eu/about

[10] https://ecs-org.eu/cppp

set up addressing issues such as Standardisation, Certification and Supply Chain Management, Market Deployment, Investments and International Collaboration, and Education, Training, Awareness, Cyber Ranges.

In the last years of H2020, following the Interim Evaluation and the Lamy report, a shift took place in EU policy thinking towards a pronounced systemic thinking, aimed at the attainment of system transformations and technological transitions. The creation of platforms able to pool EU, national and regional public investments as well as private investments and allowing for economies of scale while ensuring place-based innovation was considered critical for the attainment of the EU policy goals. Amongst other developments, it led to a **restructuring of the European Partnerships landscape** - both Public-Public (P2P) and Public-Private Partnerships (PPP).

In the field of cybersecurity, negotiations between the EC and the EU Member States were launched for the set-up of a European Partnership (PPP or P2P) on Cybersecurity, thus expanding the scope and strengthening the function of the existing cPPP.

## 2.3 The pilots

The European Commission first announced plans for the partnership in the form of a **European Competence Centre and Network** in 2018, funding pilot projects in the context of H2020 to test how such a centre and network would operate. Under the **SU-ICT-03-2018 call for proposal**,[11] consortia were invited to "*propose, test, validate and exploit the possible organisational, functional, procedural, technological and operational setup of a cybersecurity competence network with a central competence hub*".

The pilot projects, subsequently called 'Cyber Competence Network' were expected to engage in the following **activities**:[12]

- "Common research, development and innovation in next generation industrial and civilian cybersecurity technologies (including dual use), applications and services; focus should be on horizontal cybersecurity technologies as well as on cybersecurity in critical sectors (e.g. energy, transport, health, finance, eGovernment, telecom, space, manufacturing)"
- "Strengthening cybersecurity capacities across the EU and closing the cyber skills gap"
- "Supporting certification authorities with testing and validation labs equipped with state-of-the-art technologies and expertise"

These activities were expected to result in the following **impacts**:[13]

- "Cybersecurity solutions, products, or services for the identified critical challenges, increasing the cybersecurity of the Digital Single Market, in particular for sectors from which stakeholders are involved"
- "A feasible, sustainable governance model for the Cybersecurity Competence Network developed and tested through successful pilot projects addressing selected industrial challenges"
- "Clearly demonstrated strengthening of Member States' research and innovation competence and cybersecurity capacities, also within their national cybersecurity ecosystems, to meet the increasing cybersecurity challenges"

[11] EC call for proposals (2017): Establishing and operating a pilot for a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research & Innovation Roadmap. Oct 27, 20178; SU-ICT-03-2018 call for proposal

[12] Final regulation proposal / agreement 2020 "European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres"

[13] Final regulation proposal / agreement 2020 "European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres"

- "Synergies between experts from various cybersecurity domains demonstrated"
- "Bridges built between the network and industrial communities"
- "Research and Development programme with a common Research and Innovation Roadmap reflecting all different cybersecurity sectors and covering a wide range of activities from research to testing"
- "A cybersecurity skills framework model developed, which can be used as a reference by education providers to develop appropriate curricula; by employers, to help assess their cybersecurity workforce, and improve job descriptions; by citizens to reskill themselves"
- "Establishment of foundations for pooling and streamlining the development and deployment of cybersecurity technology and strengthening industrial capabilities to secure EU's digital economy, society, democracy, space and infrastructure pilots"

Four pilot projects were selected: SPARTA, ECHO, CYBERSEC4EUROPE and CONCORDIA.

These projects have a duration of around 42 months (starting at the end of 2018) and have been given an overall budget of €63.5m. The network brings together over 160 partners, including large companies, SMEs, universities and cybersecurity research institutes, from 25 EU Member States and 5 non-EU Member States.[14] Together, they account for 40% of the ECSO members.

The four pilot projects take a different but complementary approach and collaborate with each other in five focus groups to share results and experience related to Cyber ranges, Education, Governance, Road mapping, and Threat intelligence e.g., in the financial sector. The expected result of this collaboration is that the pilot projects would come to a **consolidated view** on the topics covered in the focus groups, as an input to the EC Horizon Europe work programme and the set-up of the European Cybersecurity Competence Centre and Network.

They also collaborated with the JRC by providing input for the **Cybersecurity Atlas**. The Atlas is "a knowledge management platform to map, categorise and stimulate collaboration between European cybersecurity experts in support of the EU Digital Strategy. Organisations participating in the Atlas have the opportunity to enlarge their research network, to get in contact with relevant peers, and to improve their organisation's visibility."[15]

## 2.4 The European Cybersecurity Competence Centre Network – ECCCN

### *2.4.1 Structures and roles*

In December 2020, after more than one year of preparations, the EC announced its intention to create a Cybersecurity Competence Centre Network[16] with three components: a European Cybersecurity Industrial, Technology and Research Competence Centre (ECCC), a Network of National Cybersecurity Coordination Centres (NCCCs), and the Cybersecurity Competence Community (the Community) – see Figure 2, below.

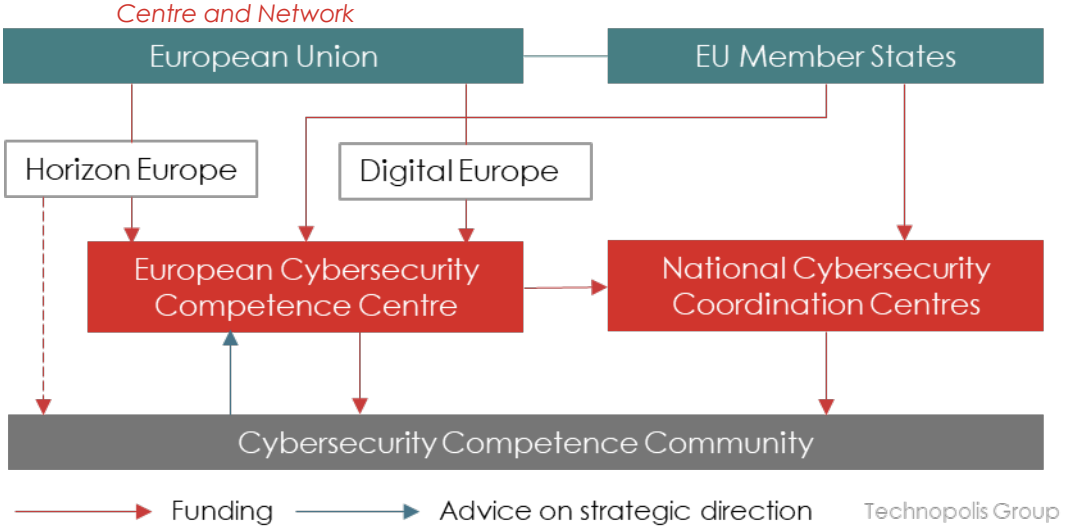
The ECCCN will be the Union's main instrument to "pool investment in cybersecurity research, technology and industrial development and to implement relevant projects and initiatives together with the Network of National Coordination Centres".[16]

[14] https://cybercompetencenetwork.eu/about/

[15] https://cybersec4europe.eu/our-community/

[16] Final regulation proposal / agreement 2020 "European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres"

*Figure 2 Structure of the European Cybersecurity Industrial, Technology and Research Competence Centre and Network*




Source: Draft Proposal for Regulation

**The European Cybersecurity Competence Centre (ECCC)**

The specific features of the **ECCC** (located in Bucharest) are as follows:[16]

- The ECCC will "implement research and innovation actions (supported by Horizon Europe Programme) as well as capacity building actions (supported by Digital Europe Programme)". Together with Member States, the ECCC will "support the build-up and procurement of advanced cybersecurity equipment, tools and data infrastructures in Europe and ensure a wide deployment of the latest cybersecurity solutions across the economy"
- The ECCC Governing Board will be composed of representatives from the Member States and the Commission. It will be in charge of adopting the Agenda (the SRIA) and the annual and multiannual work programmes deriving from it. It will have the powers "to establish the budget of the ECCC, verify its execution, adopt the appropriate financial rules, establish transparent working procedures for decision making by the ECCC, adopt its rules of procedure, appoint the Executive Director and decide on the extension of the Executive Director's term of office and on the termination thereof." The EC will "have 26% of the total votes on decisions involving Union funds, with the aim of maximising the EU value added of those decisions, while ensuring their legality and alignment with Union priorities"
- The ECCC's Strategic Advisory Group will be an advisory body on issues relevant to stakeholders, formed by the representatives of the private sector, consumers' organisations, academia, and other relevant stakeholders. The mandate will include providing "advice regarding the Agenda, annual work programme and the multi-annual work plan". The draft regulation stipulates that the strategic advisory Group "should provide advice following regular dialogue between the ECCC and the Community"

Noteworthy is that the **ECCC** is expected to have a dual function:[17]

[17] Final regulation proposal / agreement 2020 "European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres"

- On the one hand it will act as the executive entity of the 'Partnership', implementing the agreed-upon co-funded Agenda as well as facilitating and coordinating the work of the ECCCN and nurturing the Cybersecurity Competence Community
- On the other hand, it may be entrusted with the implementation of the cybersecurity parts in the Horizon Europe Programme that are not co-funded by the Member States

Its functioning will be funded mainly by the European Union. Contributions of the Member States to the resources of the ECCC can be financial and/or in-kind.

It should be noted that in essence, the ECCC will take over the mandate and functions of the cPPP in the European cybersecurity ecosystem, which will therefore cease to exist.

**The National Coordination Centres (NCCCs)**

The NCCCs should be public sector entities, or entities with a majority of public participation; they may be a national competent authority, a single point of contact, or a digital innovation hub. They will be selected by the Member States – and recognised by the European Commission as "fulfilling the capacity to manage funds so as to achieve the mission and objectives laid down in this Regulation, in accordance with the rules of Horizon Europe and Digital Europe".[17]

Criteria are, amongst other, that the NCCCs would "have the necessary administrative capacity, possess, or have access to cybersecurity industrial, technological and research expertise, and be in a position to effectively engage and coordinate with the industry, the public sector, and the research community".[17]

The NCCCs will (also) contribute to promoting and disseminating cybersecurity educational programmes, alongside relevant public authorities, and stakeholders. They will "receive direct Union financial support, including grants awarded without a call for proposals, in order to carry out their activities related to this Regulation and provide financial support to third parties in the form of grants".[18]

**The Cybersecurity Competence Community (Community)**

Based on the Draft proposal for Regulation, the Community is made up of collective bodies/organisations - including research entities, industries, and the public sector. It considers that "relevant stakeholders can be from public entities, including Member States and the European Union, as well as from industry and other entities, as well as civil society, e.g., trade unions, consumer associations, the Free and Open-Source Software community, and the academic and research community".[18]

The ECCC shall register entities as members of the Community, upon their request, and "after an assessment by the National Coordination Centre of the Member State where the entity is established".[18] Community members will not be privileged regarding the ECCC's calls for proposals or calls for tender.

The Community will benefit from the community-building activities of the ECCCN; the former is expected also to "*stimulate and support the long-term strategic cooperation and coordination of the activities of the Cybersecurity Competence Community, which would involve a large, open, interdisciplinary and diverse group of European actors involved in cybersecurity technology*".[18]

The Community will be able to provide input and advice to the ECCC by means of working groups and especially participation in the Strategic Advisory Group.

[18] Final regulation proposal / agreement 2020 "European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres"

### 2.4.2 *Characteristics and guiding principles*

The Draft proposal for regulation for the ECCCN states, "considering that the funding for the functioning of the Centre would originate primarily from the Digital Europe programme and the Horizon Europe programme, it is necessary that the Centre is **considered as a partnership** for the purpose of budget implementation, including the programming phase."[18]

Indeed, it is our understanding that the Centre and Network will constitute a hybrid of a Co-funded Partnership and an Institutionalised European Partnership (under art 185), i.e., the two forms envisaged under Horizon Europe for the implementation of EU-supported Public-Public Partnerships.

The ECCCN will be co-financed by the European Union, specifically the Horizon Europe and Digital Europe programmes, and the EU Member States. It is envisaged that the entire cybersecurity-related budget in the Digital Europe programme will be implemented through the ECCCN, while this will only partly be the case for Horizon Europe.

The description of the governance model for the ECCCN in the Draft proposal for regulation reflects several of the **rulings and expectations** set on these Partnerships in the Horizon Europe regulation[19] to be selected and co-funded as a European Partnership.

At the core are the **key principles** of transparency, openness, flexibility in implementation, and coherence and complementarity to which they are expected to adhere. Table 2 describes how these principles are related to the various components of the future ECCCN.

*Table 2 Principles of the European Partnerships and related ECCCN components*

| **Principles of European Partnerships** | **Specifications[19]** | **ECCCN components relevant for the principles** |
|---|---|---|
| More effective (Union added value) clear impacts for the EU and its citizens | • "delivering on global challenges and research and innovation objectives"<br>• securing EU competitiveness<br>• securing sustainability<br>• "contributing to the strengthening of the European Research and Innovation Area"<br>• where relevant, contributing to international commitments | • Implementation of research and innovation actions by the ECCC (supported by Horizon Europe Programme)<br>• Implementation of capacity building actions by the ECCC (supported by Digital Europe Programme)<br>• The build-up and procurement of advanced cybersecurity equipment, tools and data infrastructures by the ECCC |
| Coherence and synergies | • within the EU research and innovation landscape<br>• "coordination and complementarity with Union, local, regional, national and, where relevant, international initiatives or other partnerships and missions" | • Participation of Commission and MS representatives in the Competence centre's governing board<br>• The competence Centre's Strategic Advisory Group, consisting of relevant stakeholders<br>• National Coordination Centres |
| Transparency and openness | • identification of "priorities and objectives in terms of expected results and impacts"<br>• "involvement of partners and stakeholders from across the | • Cybersecurity Competence Community<br>• Participation of the Community in the ECCC's Strategic Advisory Group and working groups |

[19] See article 8 and Annex III of the Proposal for a Regulation of the European Parliament and of the Council stablishing Horizon Europe - the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination - Common understanding', March 2019

| Principles of European Partnerships | Specifications[19] | ECCCN components relevant for the principles |
|---|---|---|
| | entire value chain, from different sectors, backgrounds and disciplines, including international ones when relevant and not interfering with European competitiveness"<br>• "clear modalities for promoting participation of SMEs and for disseminating and exploiting results, notably by SMEs, including through intermediary organisations" | |
| Flexibility and directionality | • "approaches to ensure flexibility of implementation and to adjust to changing policy, societal and/or market needs, or scientific advances, to increase policy coherence between regional, national and EU level"<br>• common strategic vision of the purpose of the European Partnership<br>• "demonstration of expected qualitative and significant quantitative leverage effects, including a method for the measurement of key performance indicators"<br>• "exit-strategy and measures for phasing-out from the Programme" | • The Competence Centre's governing board<br>• The competence Centre's Strategic Advisory Group |

Noteworthy in the context of this study are also the following extracts of the draft proposal for regulation:

- "The Competence Centre, the Cybersecurity Community and the Network should benefit from the experience and the broad and relevant stakeholders' representation built through the contractual public-private partnership on cybersecurity ECSO, and the lessons learned from four pilot projects […] and from the pilot projects and the preparatory action on Free and Open Source Software Audits (EU FOSSA), for the **management of the Cybersecurity Competence Community**, and the representation of the Cybersecurity Competence Community in the Centre"
- "It is important to ensure respect for fundamental rights and ethical conduct in Cybersecurity research projects supported by the Centre"
- "As a result of Union contribution, access to the results of the Centre's activities and project results will be as open as possible and as closed as necessary, and re-use is possible where appropriate"
- "Due to the fast-changing nature of cyber threats and cybersecurity, the Union needs to be able to adapt fast and continuously to new developments in the field. Hence, the Competence Centre, the Network and the Cybersecurity Competence Community should be flexible enough to ensure the required reactivity. They should facilitate projects that help entities to be able to constantly build capability to enhance their and the Union's resilience"

### 2.4.3 *Functions*

The ECCCN and its components are envisioned to have the following functions.[20,21,22]

**Capacity building in the ecosystem**

- Contributing to "the reinforcement of cybersecurity and technology skills and competences in industry, technology, research and at all relevant educational levels, supporting gender balance"[21]
- Development of common training and exercises curricula. The Competence Centre will support the design and set up of specialised Masters' programmes[22]
- Provide support for SMEs by facilitating their access to knowledge and through access to the results of research and development[21]
- Engaging "with national authorities regarding a possible contribution to promoting and disseminating cybersecurity educational programmes"[21](NCCs)
- Promoting and disseminating the relevant outcomes of the work by the ECCCN at national, regional, or local level[21] (NCCCs)

**Research structuring**

- Contributing to "the enhancement of cybersecurity research and innovation, covering the entire innovation cycle, and its deployment"[21]
- "Supporting research to facilitate and accelerate standardisation and certification processes"[20]

**Community-building**

The ECCC:

- "Providing advice, sharing its expertise, and facilitating collaboration on common projects and actions"[20]
- Development of cross-sectoral research agendas[20]
- Attending relevant national, European, and international conferences, fairs, and fora, "with the aim of sharing views and exchanging relevant best practices with other participants"[21]

The NCCCs:

- Promoting, encouraging, and facilitating "the participation of civil society, industry, in particular start-ups and SMEs, academic and research communities and other actors in cross-border projects and cybersecurity actions"[21]

**Equipment and infrastructure**

- "Carrying out or enabling the deployment and facilitate the development of ICT infrastructures at the service of industries, in particular SMEs, research communities, civil society, and the public sector"[21]
- Specifically, support enabling infrastructure for security certification[21]

**Technological development**

---

[20] European Parliament. (2019). Briefing - The new European cybersecurity competence centre and network

[21] Final regulation proposal / agreement 2020 "European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres"

- "Help advance and disseminate the latest cybersecurity products and solutions across all sectors. These encompass both ICT products, processes and services and all other industrial and technological products and processes in which cybersecurity is to be embedded"[21]
- "Support the adoption and integration of state-of-the-art cybersecurity products and processes by public authorities, demand side industries and other users"[21]

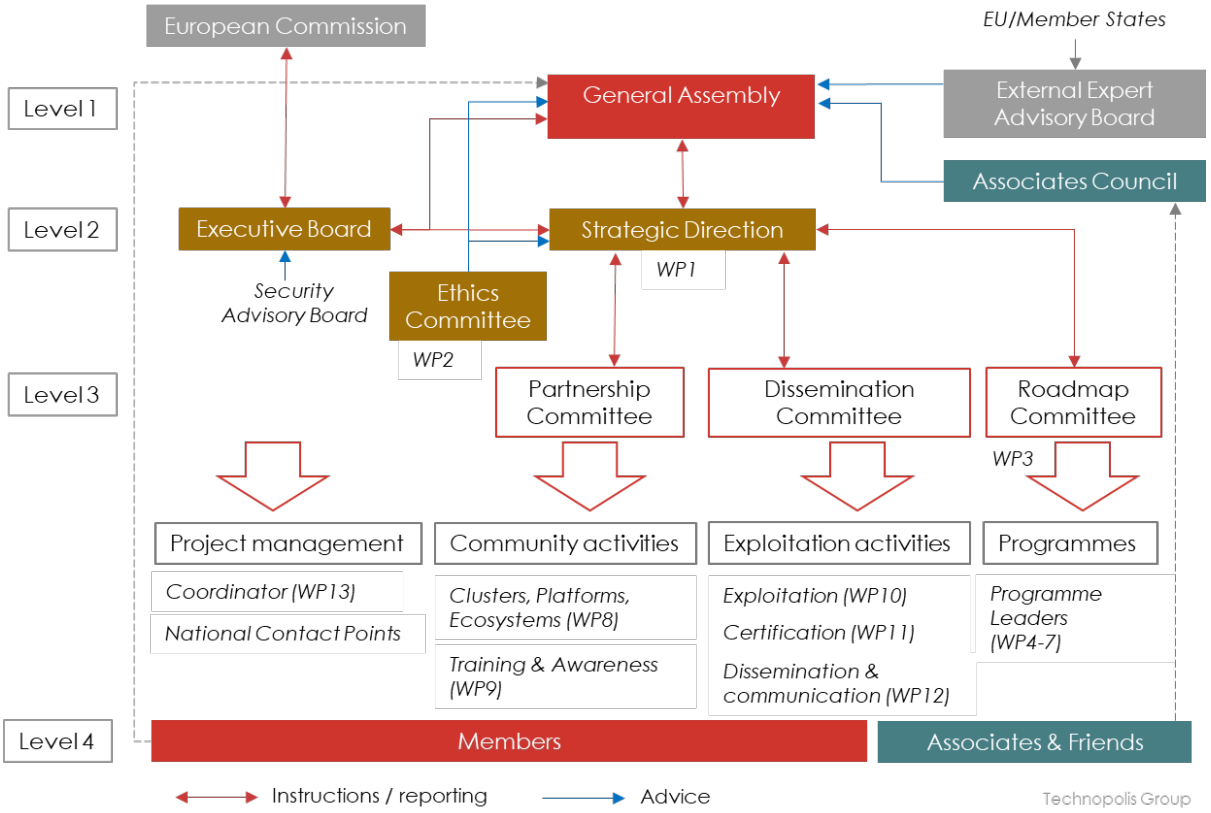
# 3 SPARTA Governance system

## 3.1 Overview of the governance and management structure

Figure 3, below, maps out the governance structure that was established for the SPARTA pilot. It shows the governing bodies and their interrelationships in the governance system.

The mapping shows the central position of the two supervisory and decision-making bodies 'Strategic Direction' and 'Executive Board', responsible for the strategy of the project and its execution (respectively).

*Figure 3 SPARTA governance and management structure*




Note: The External Expert Advisory Board is not yet established (see the Draft D1.3 report)

## 3.2 Governance principles

The SPARTA deliverable 'D1-1 Bootstrapping a CCN Pilot' informs that, in addition to formal bodies, the SPARTA governance model is rooted in concrete, applicable first principles. These principles structure the SPARTA network, guide conversations, and help navigate complex decisions. They are summarised in Table 3, below.

*Table 3 SPARTA governance principles*

| Principles | Main points |
|---|---|
| Change the philosophy of risk | The network's Roadmap and Programs will aim at identifying ambitious goals and implement research towards these goals that produce concrete and actionable results. In doing so, SPARTA is able to investigate new ideas while accurately measuring progress, promoting a "fail early, fail often" philosophy. SPARTA aims to recognize the value of negative results that successfully highlight scientific dead-ends and unfeasible technical paths. |

| | |
|---|---|
| Diversity as an asset for innovation | In a globalized digital world, SPARTA leverages geographic and disciplinary diversity to build knowledge on which to push for a more inclusive, secure and resilient European society. |
| Create opportunities for open leadership | In a fast-moving field such as cybersecurity, numerous strategic or tactical decisions need to be made efficiently. SPARTA uses these, at all levels of the network, as gender-diverse opportunities for scientists to lead the way for their communities. Such leadership requires a combination of scientific excellence, goal-driven philosophy, open-minded communication, and ethics. |
| Recognize horizontal leverage points | SPARTA recognizes the grounding importance of vertical requirement collection, and organization. These foundations are combined with a special attention to cross-domain leverage: reuse is a significant drive in the history of innovation, and it is even more effective in Computer Science where digital artefacts are easier to disseminate and adapt. SPARTA encourages horizontal developments to ensure the efficiency of its investments, maximize their impacts, and optimize their sustainability. |
| Build digital platforms for forward-looking stakeholder | The turn of the 20th century factory profoundly changed the way we produce technology. Forward-looking companies are anticipating an equivalent shift with digital platforms today. SPARTA develops and connects digital and physical platforms, as well as streamlines their related operational models. These serve as technological bases for innovation, as training facilities for cyber skills development, and more generally as catalysts and force multipliers in the development of cybersecurity capacities and digital autonomy. |

Source: SPARTA Grant Agreement – First principles

## 3.3 Governance instruments

The SPARTA deliverable D1-1 informed that the initial SPARTA proposal identified three **governance Instruments** that were needed in order to "*create a culture where the pursuit of transformative opportunities and strong international collaboration are thriving*":

- a Roadmap Instrument, which included an Associate subpart,
- a Program Instrument, and
- a Partnership Instrument.

During the project, however, the relationships established with external stakeholders has grown in importance, becoming a central 'governance' instrument.

The 'Partnership Instrument' contributes to the national, European, and international clustering activities in the project and the coordination efforts with the other 3 pilot Networks, ECSO, and EU stakeholders.

Table 4 shows the current structuring of activities and their components in terms of 'instruments' and 'enablers'.

*Table 4 SPARTA governance instruments and enablers*

| **Governance instruments** | **Enablers** |
|---|---|
| • Roadmap Instrument<br>• Programme Instrument<br>• Partnership Instrument | **Governance and Management Activities**<br>• Governance System and Components<br>• Governance Principles<br>• Roles and processes<br>• Assessment and Performance management |
| | **Transversal Activities**<br>• WP9 – Cybersecurity training and awareness<br>• WP10 – Sustainable exploitation and IPR |

| | |
|---|---|
| | • WP11 – Certification organization and support<br>• WP12 – Dissemination and communication<br>• Synergies between Programmes and Activities |

## 3.4 Governing bodies

The specific functions and mandate of the SPARTA management bodies are summarised in Table 5, below.

A committee that was mentioned in the reports and not originally listed is the **Programme Visiting Committee**. The main purpose for this committee is to support the creation of cohesion and coordination between the Programmes, as well as between the Programmes and other Community activities and Exploitation activities. It only has an indirect oversight function. The committee advises on, among others, the priorities for dissemination and exploitation, strategic research decisions, and the identification of impactful external cooperation. The representation of the Strategic Direction by the Strategic Director in the committee ensures that overall strategic decisions are aligned with the advisory activities.

*Table 5 Mandates of the SPARTA governing bodies*

| Body | Mandate |
|---|---|
| General Assembly | • ultimate decision-making body of the Consortium to which both the Executive Board and the Strategic Direction shall report and be accountable<br>• delegates executive and operational tasks |
| Strategic Direction | • supervisory body for the strategy of the Project and decision-making body of the Consortium<br>• establishes processes and frameworks<br>• mainly related to WP1, WP2, WP3, WP9, WP11 and WP12 |
| Executive Board | • supervisory body for the execution of the Project and a decision-making body of the Consortium<br>• addresses project related matters, such as interactions with SPARTA's general assembly, the European Commission and the Project Officers<br>• monitor & guide the overall work<br>• evaluate performance and results<br>• ensure the Taskforces are fully associated<br>• validate the research programmes based on the roadmap and on strategic priorities<br>• related to all WPs |
| Ethics Committee | • address major ethical, legal, personal data and societal aspects relevant to the Project<br>• address gender and diversity related topics and potential issues arising during the project implementation<br>• ensure the independency of the internal and external audits taking place during the course of the Project<br>• make the liaison with external ethics advisors, if any<br>• related to all WPs, participants recruited mainly from WP2 |
| Roadmap Committee | • propose Program Leads to the Strategic Direction<br>• design roadmap<br>• assist the Program Leads in extracting programs from the roadmap<br>• maintain roadmap |

| Body | Mandate |
|---|---|
| | • mainly related to WP1, WP3 and WPs 4-7 |
| Partnership Committee | • design and maintain network partnerships - including the Associates Council and the SPARTA workshops<br>• create and update platforms and infrastructures map<br>• coordination in serving the interests of European research and innovation teams<br>• concerned with community building<br>• mainly related to WP1, WPs 4-7 and WP8 |
| Training and Awareness Taskforce | • provide expert inputs on the state-of-the-art, gaps, and advances in the field of cybersecurity skills development<br>• provide insights on the process and tools required in these fields, and help identify potential areas of the Roadmap and Programs that can be of interest in building these capacities |
| Certification Taskforce | • provide expert inputs on the state-of-the-art, gaps, and advances in the field of cybersecurity certification.<br>• provide insights on the process and tools required in building next-generation certification tools, and helps identify potential areas of the Roadmap and Programs that can be of interest in building these capacities |
| Dissemination Committee | • provide expertise and tools<br>• monitor deliverables before publication<br>• mainly related to WP12 |
| External Expert Advisory Board (EEAB) | • advice on strategic directions<br>• review governance progress |
| Associates Council | • provide roadmap inputs<br>• suggest exploitation activities<br>• review technical and scientific progress |

Technopolis Group 2021, based on SPARTA GA documents

## 3.5 The matrix

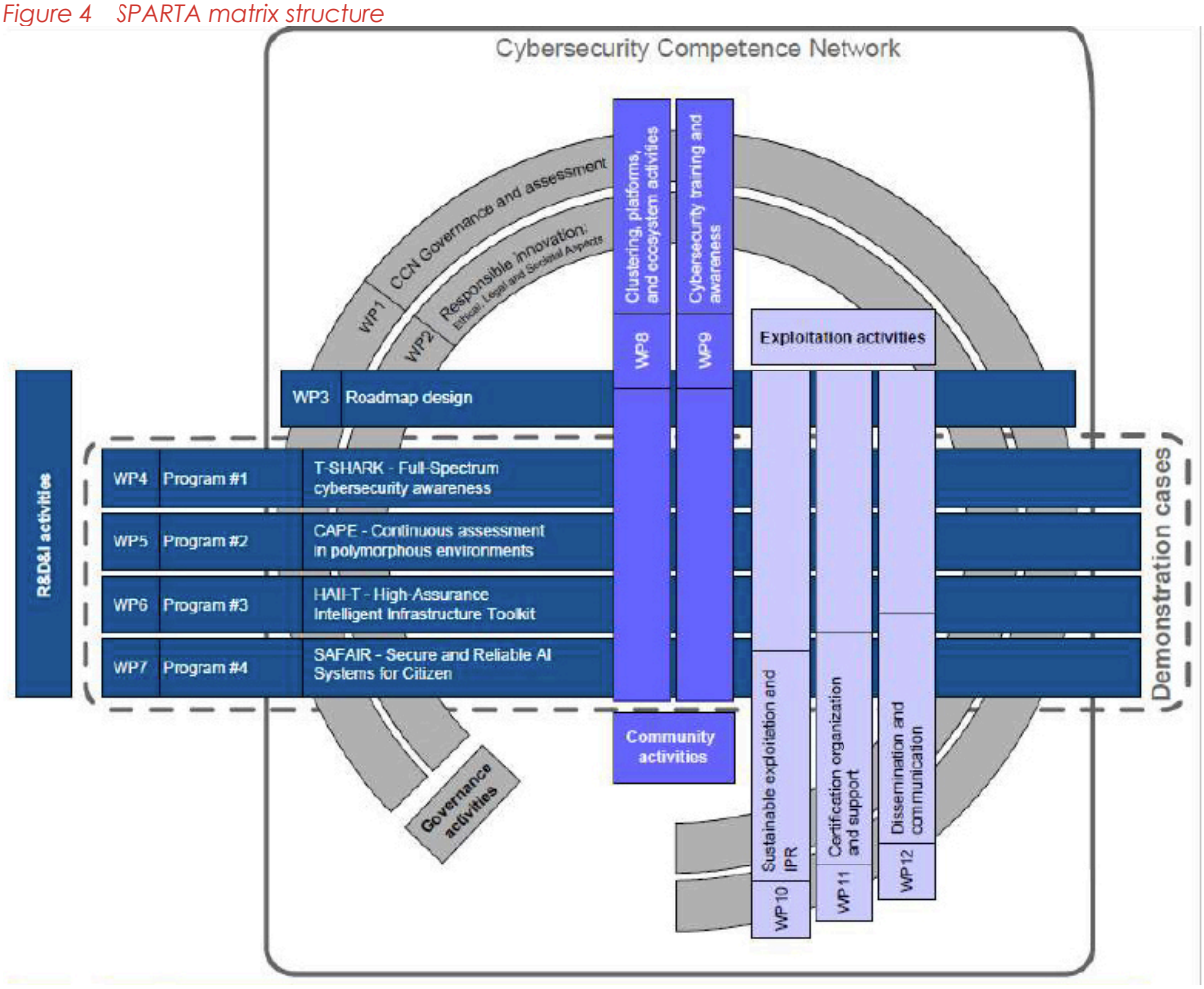
A key characteristic of the SPARTA governance and management structure is the particularly high attention for the creation of **structures and platforms for coordination and knowledge exchange** between the different WPs and areas of activities.

For this purpose, an elaborate **matrix structure** was designed, allowing for **Interactions between WPs and activities** at two levels:

- At the Network Level, between the two core governance WPs (WP1&2, responsible for the Strategic Direction and ELSA, respectively) on the one hand, and the Roadmap Design, Community and Exploitation Activities WPs on the other. In our mapping of the governance structure above, this entails coordination and interaction between the bodies and activities at Level 2 and Level 3
- At the Programme level between the Roadmap Design/Programme WPs on the one hand, and the Community and Exploitation Activities WPs on the other - in our mapping, among the bodies and activities at Level 3

In addition to the tools and platforms for the internal communication and coordination, the importance of the Partnership Instrument relates to the external interaction between SPARTA and the broader environment and stakeholders.

*Figure 4 SPARTA matrix structure*




Source: SPARTA GA – WP structure

### 3.5.1 Network level

Table 6, below, provides an overview of the participation of WP Leads or members in SPARTA's governing bodies.

*Table 6 Participation of WP leads/members in SPARTA governing bodies*

| | Strategic Direction Board | Ethics committee | Roadmap committee | Partnership committee | Dissemination Committee | Program visiting committee |
|---|---|---|---|---|---|---|
| WP1 CCN governance and assessment | X (chair) | | X | X | | X (chair) |
| WP2 Responsible innovation: ethical, legal and societal aspects | X | X (chair) | X | | | |
| WP3 Roadmap design | X | | X (chair) | | | X |

| | | | | | | |
|---|---|---|---|---|---|---|
| WP4 Program #1: T-SHARK – Fullspectrum cybersecurity awareness | X | | X | X | | X |
| WP5 Program #2: CAPE – Continuous assessment in polymorphous environments | X | | X | X | | X |
| WP6 Program #3 : HAII-T – Highassurance intelligent infrastructure toolkit | X | | X | X | | X |
| WP7 Program #4: SAFAIR – Secure and reliable AI systems for citizen | X | | X | X | | X |
| WP8 Clustering, platforms, and ecosystems activities | X | | X | X (chair) | | X |
| WP9 Cybersecurity training and awareness | X | | | | | |
| WP10 Sustainable exploitation and IPR | X | | X | | | |
| WP11 Certification organization and support | X | | | | | |
| WP12 Dissemination and communication | X | | x | | X (Chair) | |
| WP13 Project management | | | | | | |
| WP14 Ethics requirements | | | | | | |

Source: authors

The committee meetings constitute the main tool for the 'vertical' coordination between the project activities. In the monthly meetings[23] of the **Strategic Direction Board** high-level strategic decisions related to internal and external coordination are made. They thereby serve as the initial interface between external policymaking, research structuring, and third parties and SPARTA's internal bodies. All chairs of the programme-level bodies (see Table 6) participate in the Strategic Direction to ensure that overall strategic decisions are aligned with SPARTA's activities. The decisions made within the Strategic Direction are coordinated with the **Executive Board** in its monthly meetings, in which the Coordinator and all Activity and Programme leaders participate.[24] Regarding research structuring within SPARTA, the meetings of the **Roadmap Committee** are a key platform in which the roadmap process is coordinated and discussed. The committee thereby provides a '360 degrees view' on the discussions and the development of the roadmap. Apart from the WP3 Task leaders and Programme leaders, also the Activity leaders and representatives (in particular for Partnerships, Exploitation, and Dissemination), as well as SPARTA's Strategic and Executive Directors participate in these meetings. As for the community building activities, the meetings of the **Partnership Committee** serve to coordinate

[23] These meetings are held via teleconference. Up until M12 there has been a plenary meeting of the SD every six months

[24] These include all WP leaders (Governance, Ethics, Roadmap, Partnership, Certification, Training, Exploitation, Dissemination, and the four Programmes).

and manage the Partnership. The participants are a representative of CEA as SPARTA coordinator, all the partners with formal effort in WP8 and the leaders of the four Programmes. The meetings are held at least twice a year.[25]

In addition to these committee meetings, the activities in WP2 - ELSA cover all WPs. To accomplish its objective to identify and supervise relevant ethical, legal and societal aspects and challenges (ELSA), the activities engage with scholars in the SPARTA Programmes in particular. Any issues related to ELSA should be reported to the **Ethics Committee**. The committee includes all WP2 Task leaders and is chaired by the Ethics Officer, who is also the WP2 Leader.[26] Its meetings serve to supervise ELSA activities, including the ELSA Audits. One of the lessons learned in the first year of SPARTA concerned the need for alignment between the governance, assessment and ELSA frameworks.[27]

Finally, the bi-yearly SPARTA members' meetings (General Assembly) and dedicated mailing list are key tools for communication and alignment between all consortium members. The SPARTA Meetings are organised twice a year in which all project members across all Activities and Programmes are regrouped. As part of the meetings, programme and activity working sessions are organised by the Programme and Activity leaders, "encouraging bottom-up transversal collaborations".[25] Furthermore, a dedicated mailing list[28] has been created to share the news published on the SPARTA website among members and partners. This is done on a regular basis.

### *3.5.2 Programme level*

At the programme level, the SPARTA work packages, and their activities were meant to feed into each other as illustrated in Figure 5, below. The Programme-level Activities have been divided into three groups of activities:

- Exploitation Activities,
- R&D&I Activities and
- Community Activities.

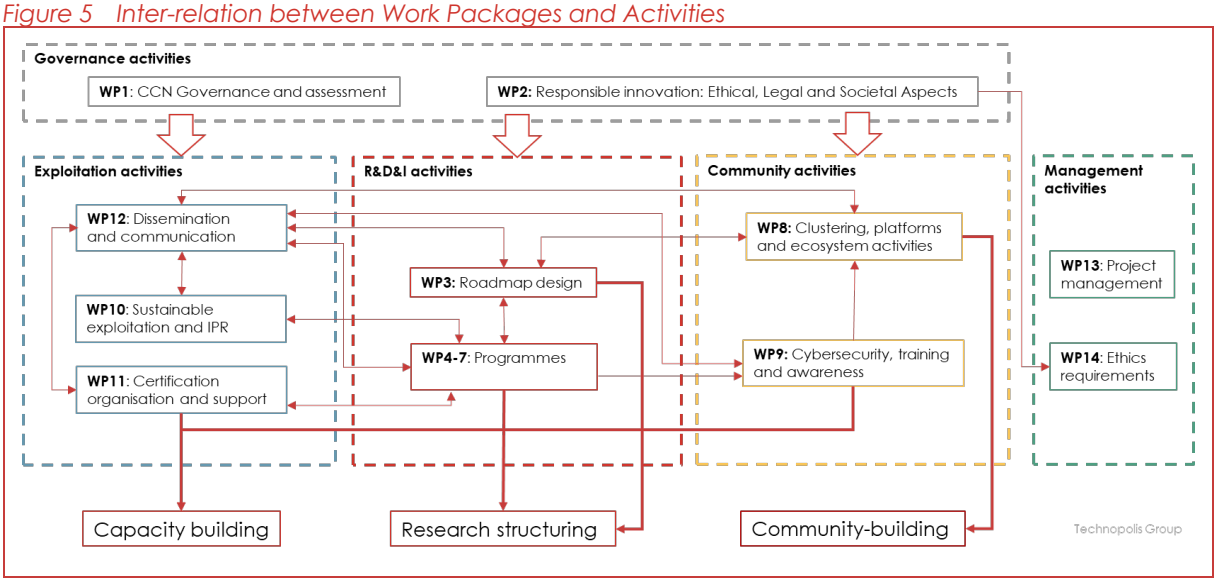
[25] D1.1 Bootstrapping a CCN Pilot

[26] To guarantee independence of the Ethics Committee, CEA is not represented in this body.

[27] D1.2 Lessons learnt from internally assessing a CCN pilot

[28] The mailing list has replaced the internal newsletter

*Figure 5 Inter-relation between Work Packages and Activities*




Source: Technopolis Group 2021, based on DOA documents

Concerning the **R&D&I Activities**, there is a continuous interaction between the Roadmap Design (WP3) and the Programmes (WPs 4-7), whereby new programme opportunities are identified through the roadmap process in WP3 and developments within the existing Programmes are fed back to the Roadmap design. These interactions take place within the Roadmap Committee and the Programme Visiting Committee. In addition, the (intermediate) results and outcomes of the Programmes are meant to feed into the Transversal Activities, by providing technical artifacts for platforms (WP8), new concepts and knowledge (WP9), insights on technologies (WP10), and insights on certification (WP11).

Regarding the **Community Activities**, WP9 (managed by the **Training and Awareness Taskforce**) provides WP8 with new training schemes and awareness artefacts. WP8 is the central Work Package that links the R&D cybersecurity ecosystem with the SPARTA network. Through this Work Package, tools and platforms are hosted to facilitate the identification of the needs within the ecosystem, that consequently feed into WP3 – Roadmap Design (see Section 3.6).

In relation to the Exploitation Activities, WP10 and WP 11 (managed by the **Certification Taskforce)** are meant to offer solutions for the Programmes concerning exploitation and IPR, and certification aspects, respectively. Furthermore, WP12 plays a key role to assess and validate dissemination and communication actions across the network. These actions are being discussed in weekly conducted brainstorm meetings of the **Dissemination Committee**. Through its communication channels, WP12 has interactions with all Work Packages, and in particular with WP1 through the introduction of Stackfield to facilitate internal communication, with WP3 and WP8 to produce communication materials for **SPARTA events** and with WP8 through the **"Go Cyber with SPARTA"** campaign.

Finally, the **Programme Visiting Committee** and its quarterly organised meetings serve as a key platform to optimise coordination and interaction between these activities, in particular between the Programmes and the other Community and Exploitation Activities. In the committee, the chairs of the Strategic Direction, the Roadmap Committee, the JCCI Group, as well as the four Programme Leads, are represented.

The deliverable D1.2 – Lessons learnt from internally assessing a CCN Pilot reported on a number of recommendations that relate to the interactions at programme level. These included:[29]

- The need to clarify the achievable level of alignment between the four technical programs on the one hand and both WP8 and WP11 on the other
- The suggestion to invest in efforts to determine whether areas of particular ELSA relevance could be located in WP5 and WP6
- The suggestion to establish trans-WP links, e.g., between WP11 and the technical programmes
- The consideration to track issues of insufficient coverage of governance aspects related to horizontal and cooperative activities

## 3.6 Interaction with the Community

The key platform for the interaction with stakeholders beyond the SPARTA consortium is the Associates Council and the community of SPARTA Associates and Friends. The Associates Council was established to serve as a platform where Associates and Friends "have an opportunity to meet and cooperate with SPARTA, proposing new ideas in a collective manner".[30] The Council convenes at least once per year and has a **Steering Committee** made of 5 representatives (either associates or friends). The platform enables the Associates to interact, and share information and resources, thereby aiming to address the fragmentation in the cybersecurity landscape, "recognising that the 44 initial SPARTA partners cannot cover all cybersecurity domains, applications, and sectors, and that additional competences are necessary."[31]

Currently SPARTA has more than 90 Associates Partners, consisting of main RTOs, industrial parties and national agencies, spread over 14 Member States. The initial network of Associates and Friends was selected by the Partnership Committee based on the needs of the network as well as expressions of interest of organisation in Europe.

The SPARTA workshops with Associate Partners constitute the main platform for knowledge exchange. In these workshops, Associate Partners have the opportunity to provide feedback to the existing Programmes and brainstorm to identify emerging Programmes. These inputs are used by the Roadmap Committee (and WP3) to update and maintain the SPARTA roadmap. In the first year, 8 workshops were organised in different European countries and by the end of the second year, the total number had reached 22.[31] The aim was to organise at least one local SPARTA event involving the Associates, each month.

Next to the SPARTA workshops, Associates and Friends can provide their feedback to the roadmap through the online **SPARTA challenge/feedback form**. These inputs are primarily used by the Programme Visiting Committee to discuss whether updates to the roadmap are necessary.[30]

Furthermore, knowledge exchange between the SPARTA network and its community occurs via the **bi-yearly SPARTA Days** which Associates and Friends can attend, and the delivery of news published on the SPARTA website to the partners through a **dedicated mailing list** (as a replacement of the internal newsletter).[32]

Finally, the **Joint Competence Centre Infrastructure JCCI** has been established to facilitate the need for cooperation and common working tools of the network and its extended community.

---

[29] D1.2 – Lessons learnt from internally assessing a CCN Pilot

[30] D1.1 Bootstrapping a CCN Pilot

[31] D8.1 Initial results of the clustering, platforms, and ecosystem activities

[32] D12.4 Updated dissemination and communication plan and evaluation

The JCCI can be accessed by both Associates and Friends. Three main components of the JCCI are planned but not yet fully operationalised:[33]

- **SPARTA WorkBench** is devoted to the integration of the computation and communication resources that constitutes a shared and distributed test-bed. The facilities should allow the sharing of this infrastructure.
- **SPARTA Virtual Learning Centre** is devoted to spread the knowledge acquired as well as for e-leaning purposes. This includes the creation of a Web Portal, its integration on the JCCI portal, and the provision of the audio/video machinery for creation, (controlled) dissemination of multimedia, information and audio/visual support for lectures and demonstrations.
- **SPARTA Cyber Range** is devoted to the establishment of the technical infrastructure for the SPARTA Cyber range. This will be based on the federation of existing cyber ranges of the partners.

In the first year, efforts focused mainly on building the framework on building a catalogue of identified platforms and tools from participants.[34]

Beyond the SPARTA Associates: the activities in WP8, but also in WP9 and WP11, focus on

- The interactions with other initiatives
- The interactions with the other pilot projects and joint workshops
- The services provided to the community in the form of education and training (cyberrange) [WP9]
- The alignment of certification support activities with the different European and national cybersecurity certification initiatives [WP11]
- The production of communication materials for SPARTA events, as well as its dissemination on SPARTA social media accounts [WP3 and WP8]
- The interactions with key institutions (EC, ENISA, ECSO, and other pilots) for the creation of a skills framework and the analysis of existing training programmes [WP9]

The key is how these interactions were meant to feed back into the SPARTA activities. For the Roadmap instrument, for example, a two-way collaboration was needed between SPARTA Partners and Associates in order to strengthen the mechanism to ensure that "*information about parallel initiatives, strategic decisions made, and other developments not known or not directly in the reach of the SPARTA Partners reach roadmap developers in timely and efficient fashion*."[35] The tools and platforms that are currently at disposal of the SPARTA consortium to allow for such 'external' collaboration and the creation of an extended competence network include the SPARTA workshops and the SPARTA challenge/feedback form, mentioned above.

Furthermore, to take stock of the cooperation synergies with external initiatives, more pro-active knowledge sharing is suggested, e.g. by making the partners "report with a small news article whenever cooperation is officially taking place".[36] These articles can subsequently be disseminated by WP12 through the SPARTA mailing list and other communication channels.

---

[33] SPARTA GA Description of work

[34] In the first year, 30 platforms and tools from 16 partners were identified. In addition, 5 online courses, 10 in person courses and 6 hands-on-labs have been gathered and provided through the JCCI website (D8.2 – Intermediate results of the clustering, platforms, and ecosystems activities).

[35] D1.1 Bootstrapping a CCN Pilot

[36] D1.3 Improving a CCN Pilot

## 3.7 Developments in Year 2

Several developments have taken place in year 2 that are relevant to SPARTA's governance structure and processes.

First, following the recommendations of the first annual project review, the consortium designed a **modular governance model**, following a matrix structure of five kinds of processes (perform, monitor, improve, synchronise, liaise) over four governance levels (network, transversal, scientific and technical, assessment).[37]

Second, the Associates Network has been further formalised, selecting a limited number (between 5 and 9) of organizations per country "to facilitate the integration in the SPARTA culture, procedures and tools"[38]. These **national clusters of Associate partners** have been tasked with identifying and selecting candidates. They will oversee coordination and represent the network in events, both at the regional and national level. Selection of new Associates is based on seeking a balance in public-private weight of a national cluster and increasing the coverage of the innovation value chain (including universities, RTOs and organisations that offer services to the end user).

Third, collaboration between other pilot projects of the competence network has been strengthened through the organisation of **inter-pilots focus groups** on which aspects related to the roadmap, governance, communication and cyber ranges were discussed, and through participation of SPARTA members to Concertation meetings.[39]

Finally, the involvement of SPARTA Associates and internal knowledge sharing was strengthened by the **extension of the JCCI to a fully distributed infrastructure**, where organisations can run their local JCCI nodes and advertise the services offered through service description languages (SDL). This allows organisations of the SPARTA ecosystem to offer directly and autonomously services/tools/data, and thereby also embody the tools developed in the Programmes. Deliverable 1.3 reports that "several tools are already used by partners and associates/friends (for instance for road mapping activities)". Regarding the governance of the JCCI structure, WP8 remains responsible for the creation of the infrastructure to host the tools and services. The other WPs are responsible for the creation of new tools/services.[40]

# 4 Assessment against the evaluation criteria

## 4.1 Effectiveness

Effectiveness refers to the extent to which the SPARTA governance structure, principles and processes were effective – as expected – in facilitating the attainment of the project objectives in relation to research structuring, community-building, and capacity-building in the ecosystem. Questions we pose to assess effectiveness of SPARTA governance are:

1) Do the governance structure, principles and processes allow for an **effective steering and coordination** of the project activities?
2) Do the governance structure and processes allow for an **effective interaction and knowledge exchange** between the governance bodies at various levels?
3) Are the governance structures and processes effective in providing interfaces and platforms for **interactions** with a variety of **relevant (external) stakeholder groups**?

[37] Source; Draft D1.3 improving a CCN pilot

[38] D8.2 Intermediate results of the clustering, platforms, and ecosystem activities (DRAFT)

[39] D1.3 Improving a CCN pilot (DRAFT)

[40] Improving a CCN pilot (DRAFT)

Before we analyse the feedback collected from the partners and external stakeholders, we make a note that significant changes were made during SPARTA's second year, following the bootstrap of SPARTA's main elements in the first year. The changes implemented included the introduction of a modular governance model, the crystallisation of the community-building activities through further extension of the network of Associates and Friends and the national clusters of Associate partners, and the full deployment of the JCCI infrastructure.

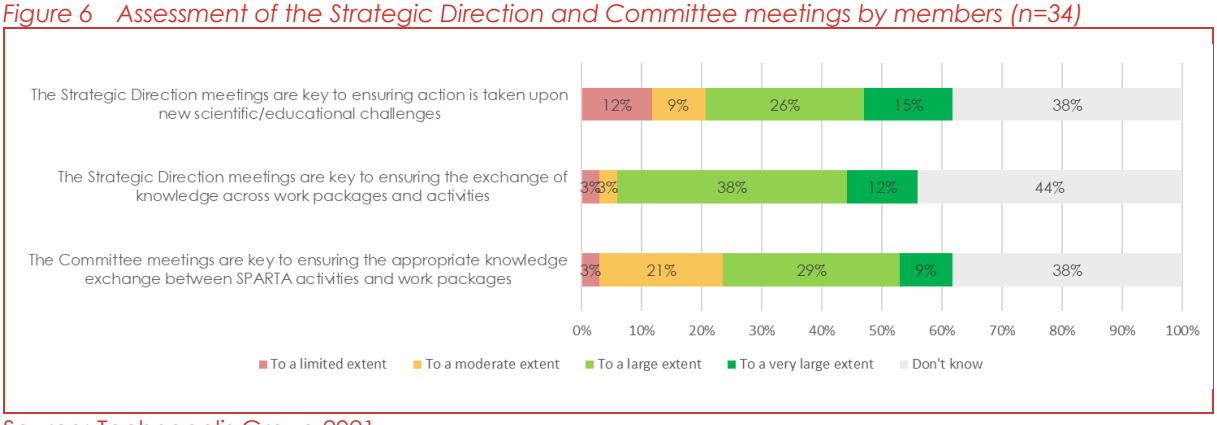
### *4.1.1 Governance structure*

As a project with a total of 44 partners and 13 work packages, the governance of SPARTA is considered challenging. In general, however, internal stakeholders view the SPARTA governance system as **effective in steering and coordinating project activities**. Most interviewees feel that currently the route of discussing issues is at the executive board level and then distributing the conclusions to the WPs works well, in particular because of the expertise of the people involved. By most it is felt that the SPARTA leadership is inclusive and open and that bottom-up ideas are encouraged. Most of the interviewees does feel that the executive board meetings are insufficient for the more practical and detailed level communication and some interviewees feel that the more junior staff is not always equally informed.

From the survey among members, it appears that most of the respondents are positive about the Strategic Direction meetings and committee meetings. In interviews with work package leaders the Executive Board meetings are mentioned often, and views are that this governance model works well. In general, there is consensus on where SPARTA is going and what direction is chosen. Interviewees also mention that the structure works well in the sense that the project was able to respond to issues raised by partners and make the necessary improvements. While at the beginning project, responsibilities of WP leaders were not always clear, the project has tried to ensure a better distribution of responsibilities and shared decision making.

According to interviewees the **distance** between the Executive Board and the Strategic Direction could be improved. This is partly because both meetings are run by different people, with the head coordinator of SPARTA only being involved in the Strategic Direction meetings. The result is that not everyone is informed about what is going on in the two fora. Only WP leaders (or someone representing them) participate in the Strategic Direction. This may explains why a large percentage of respondents has answered '*don't know*' in response to the survey questions on the strategic direction.

*Figure 6 Assessment of the Strategic Direction and Committee meetings by members (n=34)*




Source: Technopolis Group 2021

Another important aspect of the SPARTA governance is the matrix organisation. The **matrix approach** is considered to work as well as can be expected from such a large project and most interviewees see this as a sensible way of organising the project. Interviewees also mention

that half a year after the start of the project the matrix was better aligned: meetings have been consolidated and the workload of the coordinating team has been decreased. There is no micro-management.

In the interviews it was mentioned that the integration of the transversal WPs and technical WPs has been improved. Because not all partners are involved in **transversal WPs**, commitment and interaction can be difficult. For technical WPs, the requirements from the transversal WPs can sometimes be felt as a burden upon their daily work. As a solution, a platform has been built to allow for technical WPs to report only once to the transversal WPs. The next reporting cycle will use this platform. One interviewee feels that transversal WPs are also better listened to at the Executive Board meetings than before.

The people involved in SPARTA and its different work packages are considered skilled and experienced. Furthermore, the **diversity** of people and organisations involved in SPARTA is good, varied, and complementary. Of the survey respondents, 47% of the respondents finds the geographic and disciplinary diversity of the SPARTA members to be above expectations. One interviewee mentions that because of the diversity, you also need to invest more time to get to know each other, something that – because of COVID-19 – could still receive some more attention.

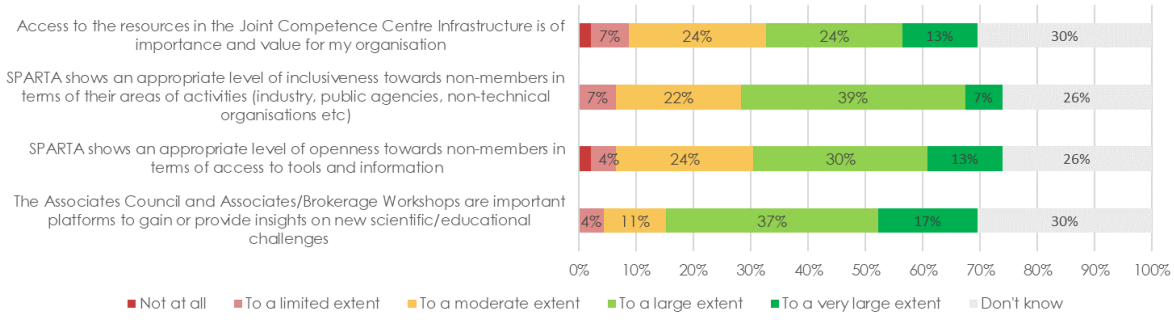
### *4.1.2 Governance principles*

Interviewees are positive about the **governance principles**, in particular the concept of changing risk, diversity and driving the European policy discussion. Several interviewees also indicate that the two audits that have taken place were a good way to be reminded of the governance principles. This has resulted in most work package leaders being aware of the principles, although not all of these find them applicable in their day-to-day WP activities. One interviewee also indicates that they would like to have tools that help them implement the governance principles in their work package.

All interviewees also considered focus on **ELSA** aspects important and something that is special about SPARTA. One interviewee mentioned that you cannot be a researcher in SPARTA and not learn about the importance of this. This is confirmed by the survey responses. 41% of respondents find the adoption of Responsible Research and Innovation and attention for ELSA throughout all activities and practices in SPARTA above expectations.

The governance principle on **openness** and **inclusiveness** are adhered to ass well. According to the survey, members and associates alike feel positive about the openness and inclusiveness of SPARTA towards non-members.

*Figure 7 Assessment of openness and inclusiveness by members and Associates/Friends (n=46)*



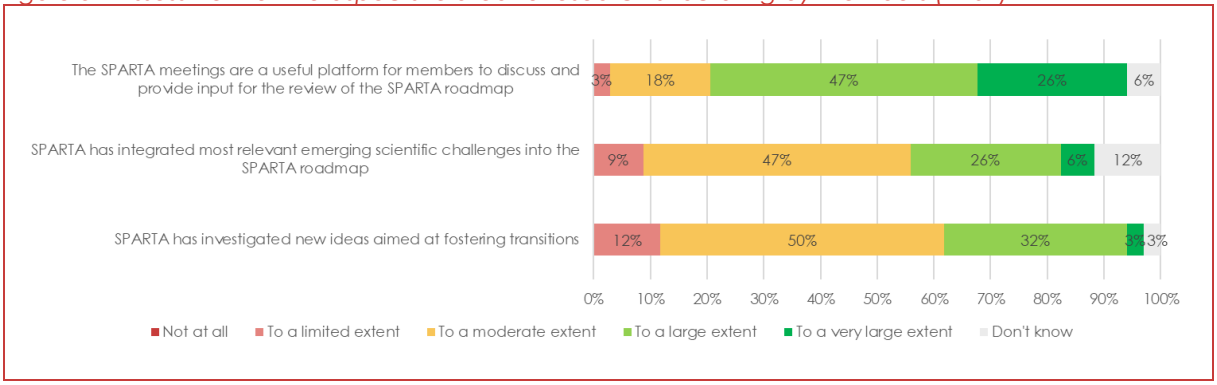

Source: Technopolis Group 2021

### 4.1.3 *Governance instruments*

All interviewees perceive the **roadmap** to be a good instrument that is responsive to changing needs and trends. Interviewees do state that at the moment, flexibility of SPARTA to respond to the roadmap is limited because of the H2020 project context. Because there is no provision in SPARTA to launch projects based on the roadmap, it is more of a theoretical exercise and not an instrument for day-to-day steering of the project. Some interviewees feel that because of this SPARTA is not as risk taking and agile as it could be. Others indicate that on programme level, there is still a lot of flexibility.

The roadmap approach can be considered an inclusive approach. According to the survey, more than 70% of the respondents find the SPARTA meetings a useful platform to discuss and provide input to the review of the roadmap.

*Figure 8 Assessment of the aspects related to research structuring by members (n=34)*

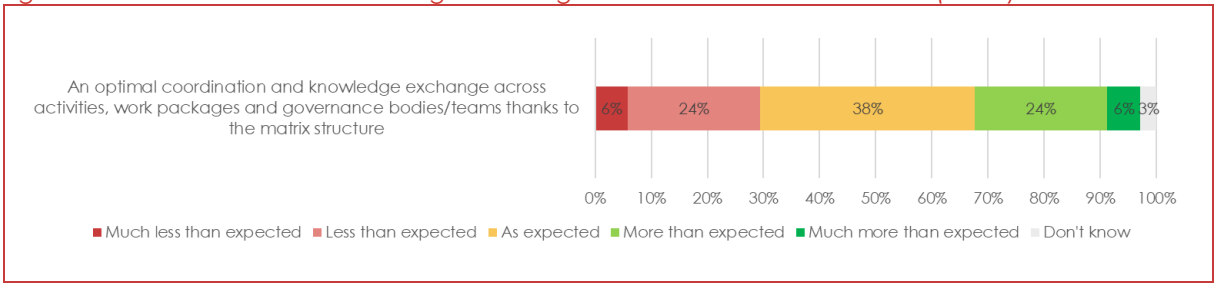



Source: Technopolis Group 2021

### 4.1.4 *Effectiveness for ensuring internal interaction and knowledge exchange*

When it comes to internal interaction and knowledge exchange, members are less positive about SPARTA's matrix structure. A significant share (30%) finds that coordination and knowledge exchange is **below expectations.** This can partly be explained by the fact that while WP-leaders feel that they have sufficient information about other WPs through the Executive Board meetings, they also feel this does not ensure sufficient integration of the different WPs. More discussion between especially the programme leaders is seen as fruitful.

*Figure 9 Coordination and knowledge exchange thanks to the matrix structure (n= 34)*

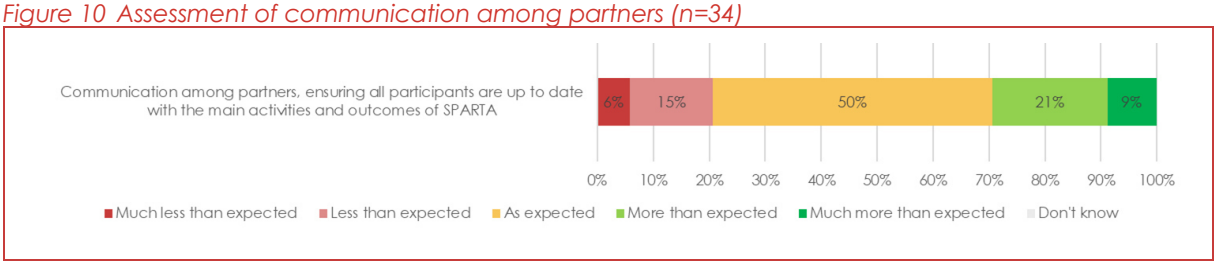



Source: Technopolis Group 2021

Some aspects of internal interaction and knowledge exchange are also hindered by COVID-19. Interviewees mention the **SPARTA days**, where all partners would meet physically, as one of the things they miss most. A total of three SPARTA days have taken place before the pandemic hit and have been replaced by a virtual workshop, but informal moments are lacking.

Overall, 50% of survey respondents finds the communication among partners to be as expected.

*Figure 10 Assessment of communication among partners (n=34)*




Source: Technopolis Group 2021

Work package leaders also state that specific efforts have been made to address internal knowledge transfer. Nevertheless, interviewees feel they cannot effectively reach all necessary people. More face-to-face interactions would be fruitful but are currently being hindered by COVID-19. Members emphasize that they try to make the online meetings as open and dynamic as possible but that for certain activities such as the development of the roadmap, the absence of face-to-face meetings is a barrier. Interviewees see a clear difference between the benefits gained from workshops and events in the first and second year of the pilot.

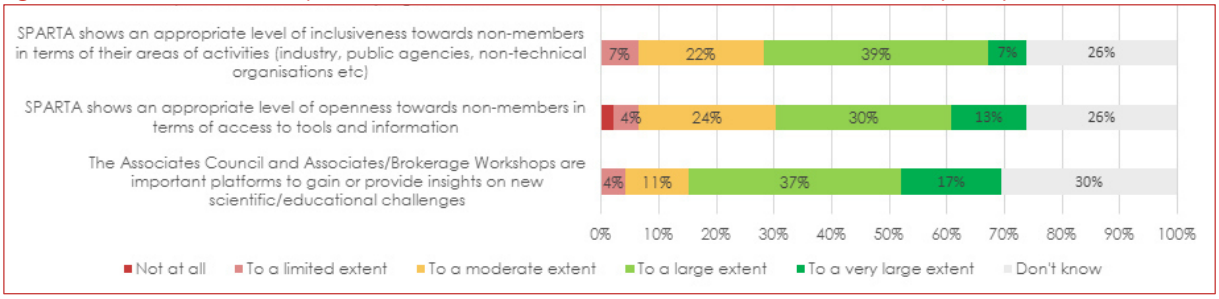
All WPs contribute to communication and have a monthly communication push. Some of the people from the technical WP's indicate that the additional communication, certification, and ELSA activities can sometimes be resource consuming. They do understand that at project level these activities are relevant and important to do but could potentially use some more guidance in this.

### *4.1.5 Effectiveness for ensuring interaction and knowledge with external stakeholders*

Internal interviewees note that external stakeholders are less involved in SPARTA than originally foreseen. However, this may not be because of lack of effort by SPARTA or lack of interest among potential stakeholders. The COVID-19 pandemic has hindered the organisation of monthly workshops with associates. For some meetings it was possible to follow-through online, for others this did not work out. Interviewees indicate that they could be involved better in future activities and that an attempt could be made to increase the number of participants.

Less than half (43% and 46%) of the partners responding to the survey feel that SPARTA is open to non-member industry actors and the geographic to a large or very large extent and disciplinary diversity of SPARTA associates and friends is good or very good. Partners feel more positive about the role of the Associate Council and the Associates/Brokerage Workshops as over 50% feel positive about them. Several respondents (26-30%) do not know if interaction with external stakeholders is sufficient, and only a small minority (4-7%) sees weaknesses interaction with external stakeholders.

*Figure 11 Assessment of aspects related to interaction with external stakeholders (n=34)*



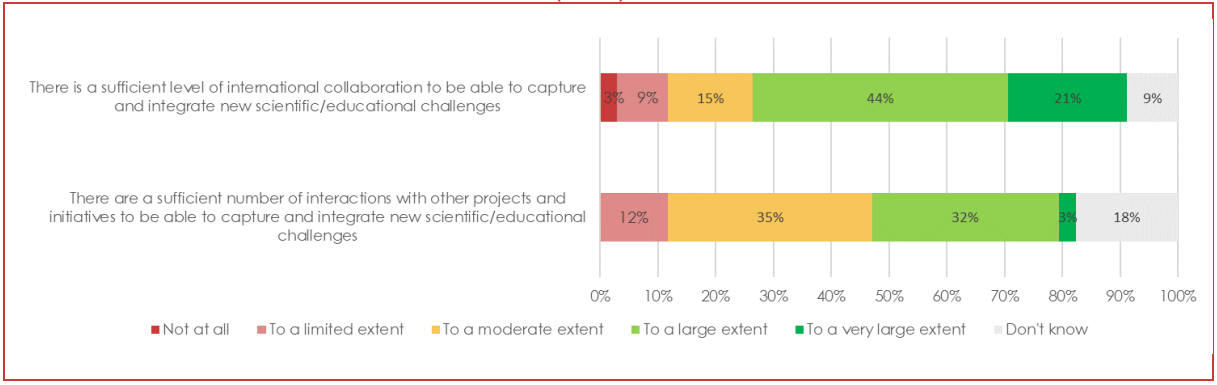

Source: Technopolis Group 2021

One interviewee does mention that an achievement of SPARTA is that is has been able to establish informal links with external partners, something that does not usually happen in these kind or large formal projects.

Initially there were plans to set up an external advisory board to get more views from outside but so far this has not happened.

Partners are rather **positive** about aspects related to capturing scientific/educational challenges through **interaction with external stakeholders** within SPARTA, 65% feel that there is a good level of international collaboration to be able to capture and integrate new scientific/educational challenges. However, only 35% feel that there are enough interactions with other projects and initiatives in view of capturing and integrating new scientific/educational challenges.

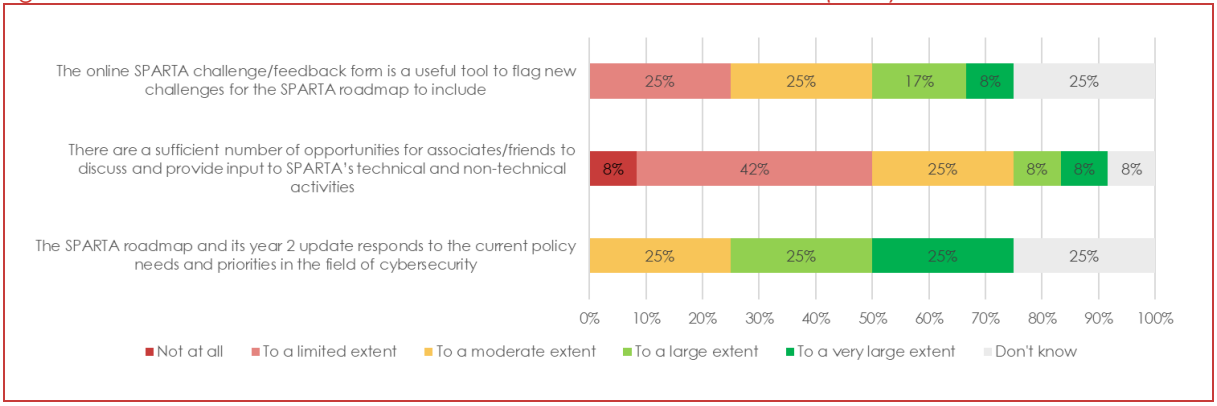
*Figure 12 Assessment of aspects related to capturing scientific/educational challenges through interaction with external stakeholders (n=34)*




Source: Technopolis Group 2021

**The associates/friends** are **much less positive** when it comes to coherence, 50% feels there is not enough opportunity to discuss and provide input to SPARTA. Furthermore, 25% feels the online SPARTA challenge/feedback form is not a useful tool and a further 25% do not know if it is a useful tool.

*Figure 13 The views of external stakeholders of interaction with SPARTA (n=12)*




External stakeholders consider SPARTA to have a good balance between end users, industry, and research organisations in their **network**. Interviewees feel that SPARTA is doing a good job in further expanding the network.

SPARTA is perceived as open and inclusive towards **associates**. Most interviewees feel well-informed and to some extent able to influence SPARTA activities. Interviewees also feel that

SPARTA is good at communicating relevant issues on a **frequent** basis. One interviewee explained that SPARTA is able to directly access their cybersecurity community. Another mentions that SPARTA reaches out asking for opinions and by sending surveys.

Based on the interviews, external stakeholders are generally very positive about the **networking activities** of SPARTA. SPARTA offers a platform for external stakeholders to present themselves to others and to get to know new potential partners, for example with other small and large companies or research organisations. It is also considered a trusted environment. The brokerage events are mentioned several times as a good example. Associate partners feel they can use SPARTA to grow their own network and establish new collaborations, also for new European projects.

According to external stakeholders interviewed, SPARTA is important in understanding where the **policies** and technologies are going in the future and is considered a good environment to discuss relevant cybersecurity themes and issues. The SPARTA **roadmap** is very relevant. Those associates that have provided input to the roadmap feel that this has been taken up.

External stakeholders refer to the challenge of raising awareness and training on cybersecurity in general. According to some of them, SPARTA is contributing well to raising awareness among SMEs, and this should also remain as a policy target in the future. **Skills and training activities** of SPARTA are much appreciated. The education map and curricula designer are considered relevant tools. The platform function of SPARTA, for others to access and explore, could be exploited more. The SPARTA self-assessment tool was mentioned as a helpful tool for raising awareness. An interviewee mentioned SPARTA contributions such as the JCCI repository and work with Cyberranges, which enable the exchange and testing of resources and tools. According to some interviewees, it is important to ensure skills and training activities of SPARTA are continued after the project ends.

External stakeholders indicate that they would like to be **more informed** about the SPARTA activities. Some feel they do not have a complete picture of what SPARTA can offer. Because of SPARTA's size and **limited available resources of the associate/friend**, it is not always possible to follow everything that is going on within SPARTA. Contact persons within SPARTA are very approachable and easy to reach by most interviewees. Some interviewees indicate that communication on EU-level could be more active.

Some external interviewees are unsure if all relevant eternal stakeholders are sufficiently engaged. Strengthening end-user engagement was also mentioned as something that could receive more attention in general, also outside SPARTA.

European-level stakeholders feel that SPARTA and the **other pilots** could be more active in their outreach, sharing information and more interaction. The fact that SPARTA is not represented in ECSO itself also complicates this. Information is shared with the individual organisations involved. Also, one associate/friend mentions that communication with the other pilots could be better coordinated and that SPARTA could also more actively share information with associates/friends.

**COVID-19** has clearly had a negative impact on the organisation of the **outreach activities**. Virtual meetings had to be organised instead of face-to-face meetings. These are considered of ok quality, but the more informal personal interactions are missed. A suggestion was also made that what (external) people do with the information they receive and whether this results in changes could also be better monitored.

The conclusion is that external interaction works well, although some of the external stakeholders see room for improvements. Based on the interviews, external stakeholders more engaged in SPARTA activities and interact more with SPARTA, generally view the benefits and interaction with SPARTA in more positive light. The more critical views seem to originate mostly from those external stakeholders with which engagement and interactions are less frequent.

## 4.2 Efficiency

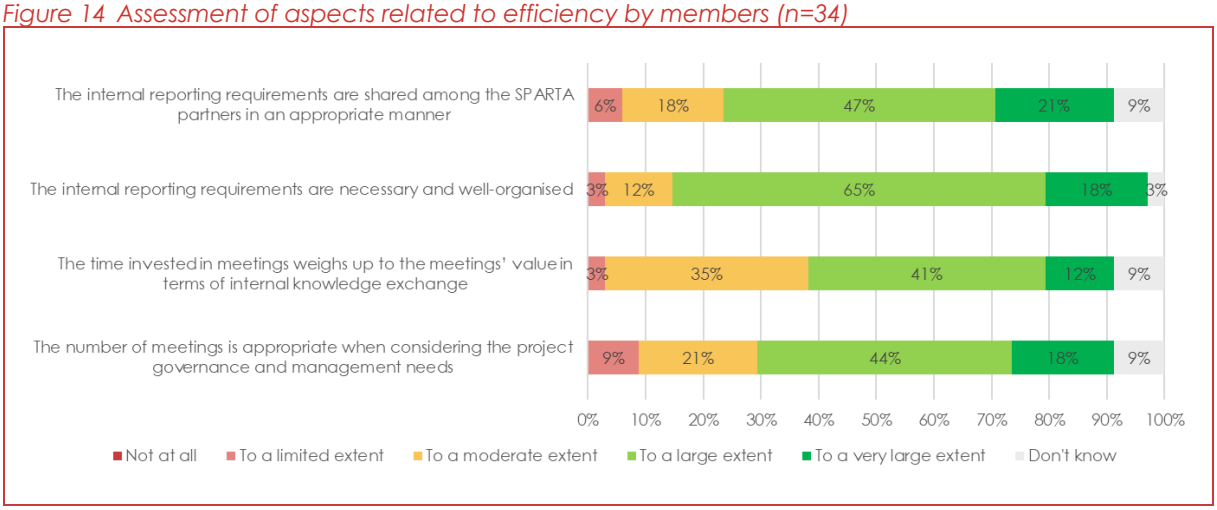
Efficiency refers to the extent to which the governance structure and processes allow for an optimisation of resource utilisation in relation to the project and programme management. The question we pose to assess efficiency of SPARTA governance is

4) Do the governance structure and processes allow for an optimisation of resource utilisation in the project implementation?

Typical consequences of using matrix structures for internal governance of large and complex projects are the **large number of meetings and reports** needed to ensure the expected communication and coordination, particularly, when combined with a strong centralised control by the coordinator. This is often reflected in critical views of partners towards time they need to use for meetings and reporting and the usefulness of these.

However, even though SPARTA governance model is based on a matrix and it has strong central coordination, the partners of SPARTA are very positive about the efficiency of SPARTA governance. Of SPARTA partners, 83% feel the internal reporting requirements are necessary and well-organised. The partners are more critical about the value of meetings. The **least positive** feedback is related to the time invested in meetings weighing up to the meetings' value in terms of internal knowledge exchange, but even there 53% see the situation in a positive light.

*Figure 14 Assessment of aspects related to efficiency by members (n=34)*




Source: Technopolis Group, 2021

The survey results are well mirrored by the observations from the surveys. Interviewees state that they have the impression that SPARTA works in an efficient manner. Most interviewees would rather increase **resources** for SPARTA governance than decrease them and add that decreasing resources would mean operations would suffer. Most feel that extra resources should go to better communication between work packages and keeping everyone informed.

Some interviewees point out that communication between work packages could be improved. Apparently attempts have been made to improve this related to reporting, but the focus has been more on communication tools and software solutions, rather than enough on the underlying governance structure and processes.

The interviewees clearly understand the need for **administration** on all activities in the context of such a large project as SPARTA. The is the only thing that according to interviewees could potentially be further streamlined is reporting. However, as the survey results clearly indicate, the general feedback related to reporting is very positive. One interviewee suggested that the European Commission or coordinators could in the future also spend more time in the

beginning of the project on training smaller organisations on the mandatory administrative requirements.

The interviews confirm that the feedback is slightly more critical towards the value of meetings compared to reporting, but still very positive.

Interviewees consider the monthly meetings of the **executive board** to be reasonable. One interviewee noted that the executive board working method is not optimal and that experimentation in governance is not facilitated to the extent expected. Another interviewee added that the setup of the Executive Board meetings does not allow for the discussion of important timely issues. Some questions were raised related to the roles of the executive board and the strategic direction board, such as are two separate boards needed as they seem to overlap, and why the coordinator seems to be more active in one, but less in the other.

Most of the SPARTA **committees** convene on an ad-hoc basis, which is considered a good thing by the interviewees. There are no regular meetings with minutes. On the other hand, one interviewee mentions that perhaps more resources could be spent on publishing meetings minutes or summaries to make the project more **open and inclusive**. The exchange between internal and with external partners could be enhanced further. Another interviewee suggests that online sessions could be recorded and broadcasted to increase the push of information about WPs and activities.

One interviewee mentioned that the **large number of partners** involved in SPARTA sometimes makes it difficult to activate all resources that were originally allocated for their WP, particularly resources planned for cross-WP activities. Nevertheless, another interviewee feels that it is an achievement of SPARTA that they have been able to bring international teams to work on research together, including very diverse partners of different types of organisations that work together in an open manner.

Several interviewees brought out the fact that the SPARTA project currently has no budget to assign to new projects, or to experiment with open calls and selecting projects. Another clear handicap in this respect is that SPARTA is implemented formally as a Horizon 2020 project with administrative framework which is much too rigid to allow the flexibility needed from a pilot action. This clearly **limits SPARTA's ability to act as a proper governance pilot** towards the ECCCN.

## 4.3 Coherence

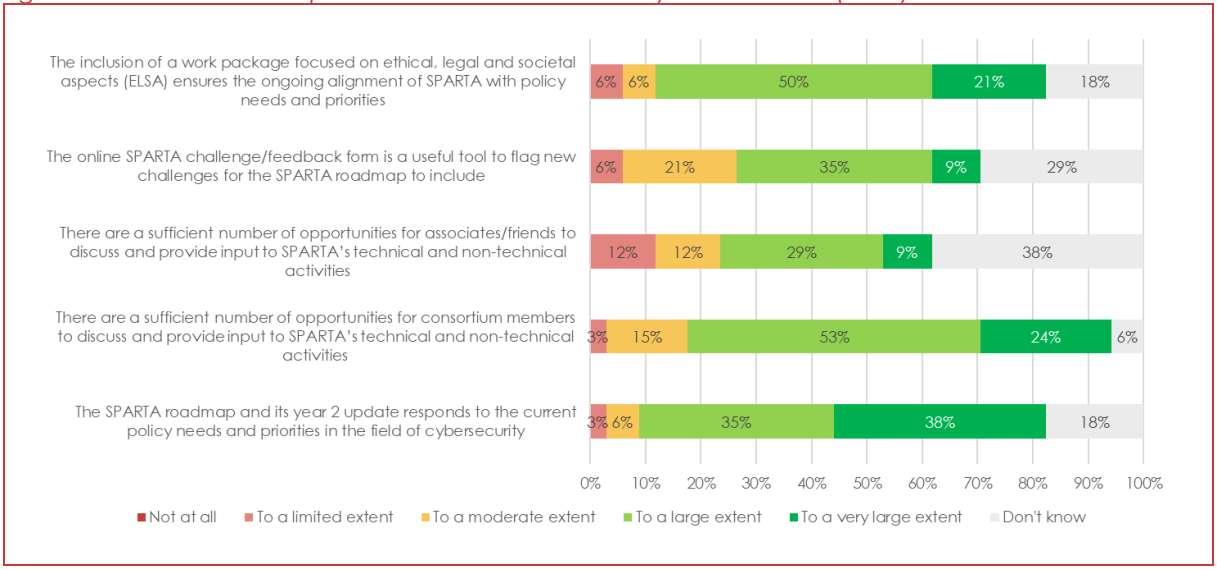
Coherence refers to the ongoing alignment of the research orientation with the policy needs and other external developments, specifically thanks to the governance structure and processes. The question we pose here to assess the coherence of SPARTA's governance is

5) Do the governance structure, principles and processes allow for an ongoing alignment of the project research orientations with the policy needs?

The 'research orientations' refer in the first place to the **roadmap design** and the 'challenges' that were picked up in WP3, as well as the extent to which WP8 (the interactions with other initiatives and the Associates) has fed into the update of the roadmap in year 2.

**SPARTA partners** are generally **very positive** on aspects related to coherence. Of partners, 71% feel that the ELSA WP ensures alignment with relevant policy needs and priorities. Furthermore, 72% feel that the SPARTA roadmap responds to the current policy needs, and 77% feel that there are sufficient opportunities for consortium members to discuss and provide input to the roadmap. However, a large percentage of partners (38%) do not know whether associates and friends also get sufficient opportunities to discuss and provide input to the roadmap.

*Figure 15 Assessment of aspects related to coherence by the members (n=34)*




Source: Technopolis Group, 2021

The picture emerging from the interviews of SPARTA partners is that the **roadmap** is open to outside trends and for example has a specific task to scan for emerging technologies. It is mostly targeted at the European Commission and national policy makers and has therefore had little impact on the work in SPARTA. Participation of roadmap committee members in networks outside SPARTA is beneficial. One interviewee suggests that the number of members in the roadmap committee should be increased from the current three.

One interviewee mentions that SPARTA offers **access and visibility** to its members as they are invited to high-level policy and scientific conferences that were not available to them earlier.

SPARTA interviewees mention that the **European Commission** keeps asking inputs from SPARTA that were originally not foreseen but do take resources and attention away from planned tasks. Others indicate that this feels as a one-way process and that they had expected more interaction with and involvement of the European Commission.

The involvement of SPARTA in ECSO is considered as important and collaboration with ENISA is considered good. People feel that SPARTA is well-positioned and has been able to build **good relationships** with relevant stakeholders.

SPARTA has **strongly connected partners** from France, Italy, and the Baltics. Other partners are less strongly connected in their national context. Also, companies are less strongly involved in SPARTA compared to some of the other pilots.

Internal interviewees feel that SPARTA members are **sufficiently aware** of relevant cybersecurity trends in Europe although the field is developing fast. One interviewee suggests that there can be a difference in understanding of threats between people in western-Europe and eastern-Europe. Most members feel they are aware of the most important trends, some indicate that direct communication of policy needs could be better, also wider than the ECCCN, for example on the Digital Europe Programme.

A side effect of the SPARTA pilot has been that funding authorities in France have launched a series of grand challenges, including on cybersecurity, which was informed by SPARTA.

Interviewees state that the **awareness** of trends in the outside world, broader than the SPARTA project itself, differs per partner. Some partners are more open to this and see the need to adapt, change and try new things while others are more focused on implementing the pre-planned/pre-defined research.

One interviewee mentions that no direct information flow is organised from the policy level to SPARTA members.

However, **associates and friends** are **less positive** when it comes to coherence. According to the survey feedback (see Figure 13), 50% of responded associates and friends feel there are not enough opportunities to discuss and provide input to SPARTA roadmap and other activities. A further 25% feels the online SPARTA challenge/feedback form is not a useful tool. This indicates much more critical view on SPARTA's activities to ensure coherence among the external stakeholders, even if we consider the low response rate (13%) among external stakeholders in the survey. Although, we must also consider that the restrictions caused by COVID-19 have prevented any face-to-face interactions during a period when significant efforts to enhance external stakeholder interaction were made. This may go some way towards explaining why the perceptions of the external stakeholders are more critical.

Some external stakeholders note that SPARTA has an important role in **facilitating learning** across sectors, especially experiences and solutions adopted by more advanced sectors.

Some also note that while the link between cybersecurity and digitalisation is very strong, less attention has been given to the possible linkages between cybersecurity and the green transition.

Most external interviewees feel that SPARTA addresses most relevant topics. For example, pushing for the development of independent resources and solutions on cybersecurity in Europe but also focusing on topics like validation and verification, GDPR compliance and explainable AI.

One interviewee notice, that the actual influence SPARTA has on **EU policies** is unknown to associates and friends. Another external interviewee does not know if SPARTA has adapted their work to policy needs and trends and see less direct impact of their activities on policy making.

According to external stakeholders, SPARTA has included emerging technologies in the **roadmap** and subsequently in the project. The roadmap is a good translation of relevant research results into observations relevant for policy and is used by several associates/friends in their own work.

Some external interviewees feel they do not have sufficient knowledge of SPARTA and its activities to actively engage and influence these activities (e.g., influencing policies or changing the roadmap).

SPARTA can identify coming **changes** well in advance, therefore there is less need to have the ability to react fast.

Some external interviewees indicate that a possible collaboration between EU-level pilots and projects, including SPARTA, could be joint **policy briefs**, also drawing from the main conclusions and lessons learned in their individual projects, presenting aspects that could be relevant for Horizon Europe, ENISA, ECSO and the ECCCN.

The impression we get about the views of external stakeholders from the interviews is somewhat more positive compared to the survey. Since the interviewees were selected by SPARTA and the survey response rate remained low, we can safely assume that the truth is somewhere between the impressions we get from the survey and from the interviews, as one is likely to be more positively biased and the other more negatively biased. In any case, the feedback is in general to the same direction, i.e., both the survey and the interviews clearly indicate that while both groups see a lot of positive in SPARTA activities directed to ensuring coherence with relevant policy needs and trends, the external stakeholders are clearly more critical than the partners, especially with respect to the ability to contribute to these activities. However, the impact of COVID-19 and especially how it has prevented face-to-face interactions should not be overlooked.

## 4.4 Relevance

Relevance refers to the extent to which the SPARTA governance structure, principles and processes **could be of relevance** as a model for the implementation of functions and activities in the future ECCCN landscape. One aspect of this is also to what extent SPARTA governance model is aligned with the principles set out for the Horizon Europe European partnerships. The question we pose to assess the relevance of SPARTA governance is:

6) Which elements of the SPARTA governance practices can be of relevance for the components of the forthcoming European Cybersecurity Competence Ecosystem?

We approach this question through the interviews with partners and external stakeholders. Many of the interviewed partners state that the **ECCCN was a surprise to SPARTA partners**. While the **European Commission** has invited them to comment on the ECCCN on some occasions, there is a feeling not much can be changed from the direction the EC has taken. One external interviewee indicated that SPARTA has informed them on the opportunity of becoming a member of the local NCCC and raised their awareness about the coming ECCCN.

### *4.4.1 Governance principles*

One interviewee encourages the ECCCN to remain **open** and maintain dynamic communication **across regions**, **cross-domain** and **cross-sectoral**. The open governance approach that is part of WP1 could enable this. Another good example mentioned in the interviews is open-source platforms.

The **circles of trust** approach with partners, associates and friends to governance is seen as an appropriate model for the ECCCN.

Something that has not yet been tackled within SPARTA but should be part of the ECCCN is resolving the issues of keeping everyone aware of the relative **importance and urgency** of identified issues, so that these can be prioritised and addressed in a timely manner.

**Cultural issues** need to be considered in the coming ECCCN context, particularly how to manage big differences in mind-sets, e.g., formal vs. informal interactions and networks, and closed vs. open access to results, resources, and tools.

### *4.4.2 Governance structure*

Several interviewees feel that the **SPARTA governance structure** is appropriate model for the ECCC. The location of the ECCC in Bucharest is a bit more difficult for the SPARTA consortium, as they currently do not have a partner in Romania. Furthermore, the management of research funds is currently not part of SPARTA, which limits its possibilities to act as a proper pilot towards key functionalities planned for the ECCC. Some interviewees feel that SPARTA is particularly relevant for managing the community and the interaction between the ECCC and the national centres.

The SPARTA advisory group consisting of experts and end-users is considered a good approach that could be beneficial for the ECCCN.

### *4.4.3 Tools and resources*

Interviewed partners feel that **tools** developed in the SPARTA project should at some point be published outside the project and transferred to independent platforms to ensure a wide reach and sustainability. When SPARTA stops, relevant tools should remain. Ensuring access to the **SPARTA tools** after SPARTA ends is also important for external stakeholders. A shared platform with access to tools such as the self-assessment, basic training material and up-to-date information on relevant information on policy needs and common threats was suggested by one interviewee. The SPARTA approach of establishing a common **repository** can be a good starting point.

The SPARTA work on **skills and education** is seen relevant for the community. SPARTA has invested in developing solutions regarding cybersecurity **skills and competences**. The CYBERWISE.EU training and the cyberrange environments are mentioned as good examples. Take this into account in the new structure, recognising the need for new skills and competences and perhaps linking it to ERASMUS plus and the skills pact objectives.

The practical support programme SPARTA provides for the involvement of **young females** is suggested as a good practice for the ECCCN.

#### *4.4.4 Roadmap*

The SPARTA **roadmap approach** is seen relevant for ECCCN and particularly the per-annual activity on keeping this updated and looking for new challenges is something that could be adopted. It is a tool that enables the identification of the most important developments and white spots in the European cybersecurity landscape and the speed with which developments are happening asks for regular updates of the roadmap.

External interviewees suggest that a high-level European **roadmap** should be established, with local and more distributed implementation. Activities based on the shared roadmap should be flexible and experimentation should be possible. One internal interviewee adds that Europe currently does not have industry leaders and that to make the necessary advances in Europe requires risk taking, experimentation and allowing failure to happen.

The **roadmap approach** of SPARTA, building on strong competences and working with periodical updates, is also considered to work well and something that could be followed in the future. Important is that the wide community is involved in this process. The educational map is considered very practical as well, potentially merged with similar activities performed e.g., by the CONCORDIA pilot.

#### *4.4.5 User engagement and exploitation*

The SPARTA **exploitation activities** are considered to allow for the definition and construction of real-life user cases and projects. Particular references in this respect were made to the SPARTA Brokerage Events.

#### *4.4.6 Outreach*

Several interviewees indicated that the proactive approach adopted by SPARTA to expanding the network of associates and friends and communicating with them was appreciated. While there were also critical views, these came mostly from associates and friends with less engagement and direct contacts to SPARTA activities.

Continue the **proactive communication** with the community and the organisation of big networking events, ensuring the community and network is active and informed. The network should stay **open and inclusive** towards external stakeholders. Ensuring a trusted environment for this is key to enable learning from both good and bad practices. The current European cybersecurity landscape is still considered to be fragmented.

#### *4.4.7 Other observations*

Interviewees feel that the **cross-pilot** working groups could function better. This is partly because the pilots have a different understanding of the concept of governance but also because people are reluctant to share information with each other, while activities conducted in other pilots could be relevant for WPs in SPARTA. However, survey respondents are **positive** about the interaction with other pilot projects (47% to a large or very large extent), which might be linked to the very active and well-functioning cross-pilot communication group.

Compared to the **other pilots**, SPARTA is seen as more open and focused on research. It is also more closely dealing with ICT standards. According to some interviewees, communication

could be even better though, and one interviewee feels CONCORDIA is better at the inclusion of new partners, also in the governance.

The cybersecurity **community** must find ways to self-organise, now that the new approach is driven by public sector entities instead of the current ECSO and 4 pilots that are **bottom-up** networks built by the community actors themselves. The ECCCN should also seek to benefit from the different networks active in Europe and developed by the community and to try and maintain the open community approach that currently exists. One interviewee is afraid that there will be a gap between closing the four pilots and the new structure being up and running. This gap might result in losing momentum. It is important to ensure that the community and particularly companies and end users can be engaged into the community in a meaningful way without major gaps.

The four pilots should make clear recommendations on how the ECCCN should be governed.

An opportunity for SPARTA and the ECCCN that was mentioned in one of the interviews is the **Horizon Result Booster** for disseminating project results. It enables EU projects to work on their dissemination strategies together and could be a way to improve the communication of the four pilots.

### *4.4.8 Alignment with EU partnership principles*

Table 7 shows the analysis of the alignment of SPARTA governance activities and principles against EU partnership principles. The relevant conclusion is that except for sufficient levels of flexibility needed for a proper pilot in the context of the ECCCN, SPARTA is very well aligned with the EU partnership principles, both with respect to its governance principles and its activities.

*Table 7 Alignment of SPARTA principles and activities with EU partnership principles*

| EU Partnership principle[41] | SPARTA principle | Activity in SPARTA |
|---|---|---|
| More effective (Union added value) clear impacts for the EU and its citizens<br>• delivering on global challenges and research and innovation objectives<br>• securing EU competitiveness<br>• securing sustainability<br>• contributing to the strengthening of the European Research and Innovation Area<br>• where relevant, contributing to international commitments | Change the philosophy of risk (ambitious goals, new ideas, concrete actionable results)<br>Create opportunities for open leadership (multicultural, gender balanced)<br>Recognize horizontal leverage points (cross-domain)<br>Build digital platforms for forward-looking stakeholder (concrete assets for future) | SRIA/roadmap – WP3<br>Research programmes – WP4-7<br>Sustainable exploitation and IPR – WP10<br>Certification organization and support – WP11<br>Dissemination and communication – WP12 |
| Coherence and synergies<br>• within the EU research and innovation landscape<br>• coordination and complementarity with Union, local, regional, national and, where relevant, international initiatives or other partnerships and missions | Diversity as an asset for innovation (geographical)<br>Create opportunities for open leadership (multicultural, gender balanced)<br>Recognize horizontal leverage points (cross-domain) | SRIA/roadmap – WP3<br>Responsible innovation: Ethical, Legal and Societal Aspects – WP2<br>Clustering, platforms, and ecosystem activities – WP8<br>Cybersecurity training and awareness – WP9 |

[41] Proposal for a Regulation of the European Parliament and of the Council stablishing Horizon Europe - the Framework Programme for Research and Innovation, laying down its rules for participation and dissemination - Common understanding', March 2019

| EU Partnership principle[41] | SPARTA principle | Activity in SPARTA |
|---|---|---|
| | | Certification activities – WP11 |
| Transparency and openness<br>• identification of priorities and objectives in terms of expected results and impacts<br>• involvement of partners and stakeholders from across the entire value chain, from different sectors, backgrounds, and disciplines, including international ones when relevant and not interfering with European competitiveness<br>• clear modalities for promoting participation of SMEs and for disseminating and exploiting results, notably by SMEs, including through intermediary organisations | Diversity as an asset for innovation (geographic, disciplinary)<br>Create opportunities for open leadership (multicultural, gender balanced)<br>Recognize horizontal leverage points (cross-domain) | Responsible innovation: Ethical, Legal and Societal Aspects – WP2<br>SRIA/roadmap – WP3<br>Clustering, platforms, and ecosystem activities – WP8<br>Education & awareness activities – WP9<br>Dissemination and communication – WP12 |
| Flexibility and directionality<br>• approaches to ensure flexibility of implementation and to adjust to changing policy, societal and/or market needs, or scientific advances, to increase policy coherence between regional, national and EU level<br>• common strategic vision of the purpose of the European Partnership<br>• demonstration of expected qualitative and significant quantitative leverage effects, including a method for the measurement of key performance indicators<br>• exit-strategy and measures for phasing-out from the Programme | Change the philosophy of risk (test, pilot, fail early, fail often, value of negative results)<br>Diversity as an asset for innovation (geographical, disciplinary) | CCN governance and assessment – WP1<br>SRIA/roadmap – WP3<br>Project management – WP13<br><br>*Note: The levels of flexibility needed for a network governance pilot towards a new European landscape is not possible to achieve in the administrative context of a Horizon 2020 funded project.* |

Source: Technopolis Group, 2021

### 4.4.9 *Relevance of SPARTA key performance indicators in view of the ECCCN*

The analysis of SPARTA key performance indicators (KPI) is described in more detail in the Annex. Table A1 analyses the relevance and appropriateness of SPARTA KPI against the role of SPARTA as a pilot towards the coming ECCCN. Furthermore, the same table looks at the relevance and appropriateness of SPARTA KPI against the needs of the future ECCCN, and its key actors ECCC, the NCCCs, and the Community. Table A2 complements this by analysing the relevance and appropriateness of SPARTA KPI against the objectives of the original call.

The overall conclusion of this analysis is that while the SPARTA KPI cover most of the relevant objectives of the original call and objectives of SPARTA, the relevance and appropriateness of many of the selected KPI are only limited. First, the selected KPI provide little insight into the nature of SPARTA as a governance pilot, e.g., to what extent alternative governance arrangements have been tested and assessed, or to what extent new observations from the roadmap work have resulted in changes into the work plan. One explanation to this might be in the Horizon 2020 project context, which does not allow the necessary flexibility needed in a governance pilot.

The KPIs defined for monitoring SPARTA objective 1 are weak. Only one of the defined KPIs can be regarded as moderately relevant (#1.3), and even that is more suitable for monitoring changes in satisfaction rather than governance quality.

Another weak area is related to the interaction with the other pilots. Only one indicator is defined for collaboration with other EU and national initiatives (#3.2) and even that does not differentiate sufficiently between different types of collaborations. This may be due to the original set-up, where the four pilots were launched as competitive efforts.

The KPI defined for SPARTA objectives 2, 3, 4 and 6 are mostly relevant and appropriate. However, some of these should be further developed to improve their relevance. For example, mere event participation or sending information and visiting web pages cannot be regarded as a sufficient indication of increased awareness and knowledge (#6.3, #6.4).

The KPI defined for SPARTA objective 5 could and should be developed further. The KPI refer to highly important assets. However, developing KPIs related to these assets must be based on clearly defined quantitative objectives, and linked as directly as possible to the contribution of the measured action, in this case the SPARTA project. Also, number of technologies depends on how a technology is defined differentiating it from other technologies. Also, some technologies are often more valuable than others, so the number may be less important than the value. Both aspects should be very clearly defined.

KPI defined for the SPARTA objective 7 are relevant and appropriate for measuring the impacts of the action. However, they are and indirect and only moderately relevant for measuring the impact of SPARTA as a governance pilot.

Table A2 shows that SPARTA KPI cover all the original objectives of the call. Comparing the SPARTA KPI to the presented examples of possible good indicators, there are several areas where the KPIs could and should be further developed. Many of the call objectives refer to impacts where it would be relevant and appropriate to measure the contribution of the action (i.e., SPARTA) to the number of projects and funding volumes allocated to selected topics mentioned as relevant in the original call. The SPARTA KPI could be improved in this respect.

Another area for development is also relevant to the future ECCCN. This is related to the measurement of impacts of activities aimed at increasing awareness, knowledge, and competences in the community and in general. SPARTA KPI rely on the typically used indicators focusing on participation, interaction or simply informing, which cannot be regarded as a sufficiently reliable indicator of real impact. Efforts should be made in future to develop better indicators based on models which define the different levels of awareness, knowledge, and competences, like the Technology Readiness Levels. These models could be developed into web-based self-assessment tools, surveys, etc. to further promote awareness, knowledge, and competences, and data collection for more relevant and appropriate indicators.

# 5 Conclusions and recommendations

This section summarises the main conclusions based on our observations during the assessment of effectiveness and efficiency of SPARTA governance and how it ensures coherence with relevant policy needs as well as European and global cybersecurity trends.

The summary is followed by recommendations aimed at supporting the implementation of SPARTA during the final year and issues related to their implementation. The section ends with our observations concerning the relevance of SPARTA experience to the future ECCCN landscape. It is aimed at supporting the identification and adoption of SPARTA experience by the key actors of the new ECCCN landscape, i.e., ECCC, the NCCCs, the EU Commission, and the Cybersecurity Community networks.

## 5.1 Conclusions

Overall, SPARTA governance model and how it is implemented does not seem to have any specific serious weaknesses. It is effective and efficient, and it has been able to ensure that SPARTA activities are well aligned with the relevant policy needs and cybersecurity trend. Hence, there is no need for radical action

The main strengths of the SPARTA governance are listed in Table 8.

*Table 8 Main strengths of SPARTA governance*

| **Strengths** | **Notes** |
|---|---|
| Matrix governance structure seems to be the viable approach for SPARTA | While the matrix approach as known inherent challenges especially related to internal communication and knowledge exchange, SPARTA has apparently been able to make is work rather well |
| Governance principles and ensuring their implementation in practice: openness and transparency, concept of risk, and diversity | Even though SPARTA has not been able to explore and implement a new concept of risk fully (e.g., fail often, fail fast) because of the Horizon 2020 project administrative context, the principle itself is appreciated. While further improvements are always possible, partners as well as associates and friends appreciate SPARTA's diversity and openness. Audits are seen as a good way to remind about the principles and thereby ensure their implementation. |
| Proactive approach and inclusion of associates and friends, the tiers-of-trust approach | Associates and friends appreciate SPARTA's proactive approach to expanding the network, informing about new developments and opportunities, and engaging users with researchers. The Associates Council and the Brokerage Events are most positively referred to as well as the frequent proactive communication. |
| Roadmap work | Partners as well as associates and friends all feel that the SPARTA roadmap is very well aligned with all relevant policy needs and global cybersecurity trends. Furthermore, the periodical updates to the roadmap are seen as valuable. |
| The JCCI repository | Despite the obvious limitations as not all actors are willing or able to be equally open and transparent, the repository is seen as a good approach and starting point even beyond the SPARTA project for establishing shared resources and tools for the European cybersecurity community. |
| Balanced network of relevant actors from research, industry, government, and civil society | The proactive expansion of the SPARTA network nationally and in Europe has developed a well- |

| | |
|---|---|
| | balanced network of relevant actors representing the European cybersecurity community. |
| SPARTA activities and the network as a platform for identifying new partners and project ideas | SPARTA partners as well as associates and friends see SPARTA activities and the network a good platform to identify and discuss common interests, as well as identify potential new project ideas and consortia. |
| Support for awareness raising, competence development, and training | While some of the other pilots are even more strongly focusing on competence development and training, associates and friends view SPARTA activities particularly in supporting the assessment and raising of staff awareness valuable. |
| SPARTA governance is efficient | Despite some smaller concerns related to the value of meetings, the general feeling is that SPARTA governance is efficient and instead of pointing to anything unnecessary, the general feeling is that even more resources could be allocated to governance. |
| SPARTA active collaboration with the other pilots | While more could and should be done, the work with the other three pilots especially in communication and also with respect to the roadmap is appreciated. |

Source: Technopolis Group, 2021

How these strengths and the underlying approaches may be translated and adopted in the new landscape is discussed later in connection with the observations related to the ECCCN.

Besides apparent strengths, the assessment has also revealed potential areas of governance where improvements may be possible. These are listed in Table 9. The focus is on SPARTA's ability to act as a pilot towards the ECCCN landscape.

*Table 9 Potential areas for improvement*

| **Potential areas for improvement** | **Notes** |
|---|---|
| Limited opportunities and possibilities to act as a real pilot towards the ECCCN | This is a weakness of launching the pilots under the Horizon 2020 project administrative context, not SPARTA. This refers two main issues particularly. First, similar governance in the ECCCN landscape is responsible also for allocating funds for cybersecurity research. This would have required a separate budget allocation for new projects, which was not available. Second, a pilot should experiment with an adaptive research portfolio based on roadmap changes, i.e., making changes to the work plans of the technical work packages. While this may not have been viable for several reasons, this would increase SPARTA's value as a pilot towards the ECCCN. |
| Internal interaction between WPs | While everyone understands the challenges of governing a matrix of technical and transversal activities, improvements in internal interaction are possible and should be done. Recognising that efforts have already been made, the focus in further improvements should be more on the contents and effectiveness of interactions rather than tools. |
| Internal interaction vertically | SPARTA approach is very much top-down, which means issues often need to be escalated to the executive committee. While this is good and necessary in ensuring that all relevant actors have a chance to discuss issues openly and decision-making is transparent, this places an extra communication |

| | |
|---|---|
| | burden to the WP leaders to keep themselves and all relevant people contributing to their WP informed about issues. Partners with no WP to lead are especially reliant on WP leaders in this respect. |
| The respective roles of the executive and the strategic direction boards | It seems to be unclear even to the partners why there are two different committees which seem to deal mostly with same issues, and why the coordinator is less active in the executive committee. |
| Interaction with associates and friends | While the main reason for limited interaction between associates and friends and SPARTA is most likely the lack of engagement of associates and friends themselves, more effort could be considered by proactively targeting the less active associates and friends. In most cases the perceived added value of SPARTA to the associate/friend largely explains their engagement and activity towards SPARTA. Being able to communicate SPARTA potential added value may increase activity and engagement. Hence, this should only be done in cases where clear added value can be communicated. |
| Associates and friends feel they have limited possibilities to influence SPARTA activities<br>The challenge/feedback collection form is not optimal for data collection | SPARTA could be more transparent by showing what external inputs they have received and how these are being used to shape SPARTA activities. For example, SPARTA could publish summaries of stakeholder consultations to the stakeholders with clear messages how the collected views will be used.<br>The challenge/feedback form should be further improved. |
| External advisory group | This was seen in the original plans, but not implemented. SPARTA should consider setting one up, possibly together with the other pilots. |
| Collaboration with the other pilots | While efforts and positive progress has already been made, further efforts are necessary to ensure that SPARTA experiences can be learned from in view of the future ECCCN structure. |

Source: Technopolis Group, 2021

It should be noted that some of the areas for improvement have emerged partly because of the unforeseen limitations to physical face-to-face interaction caused by the COVID-19 pandemic. At first, it was thought that the pandemic will be over soon, so activities were simply delayed. Once it became obvious that the pandemic will be of longer duration, activities were launched virtually. While many activities can be implemented fully virtually, virtual interaction tools cannot facilitate all forms of informal face-to-face interactions normally taking place in various configurations over coffee breaks, lunches, dinners, and drinks. This has had an impact on the quality of interactions as well as caused delays and making it more difficult to launch new collaborative activities. While SPARTA has been managing as well as can be expected under the circumstances, the clearly negative impact of COVID-19 especially on interactions and consequences of it should not be ignored when making conclusions about SPARTA governance.

## 5.2 Recommendations for SPARTA

While there are no immediate needs to address any serious inherent weaknesses in the SPARTA governance, there are areas where governance could be further developed and improved. The assessment has identified issues related to governance bodies, internal communication, outreach, and external communication, and SPARTA's value as a governance pilot. The

following discusses and makes recommendations how these issues may be addressed and further developed during the final year of SPARTA and in view of any related continuing activity.

### *5.2.1 Clarify the role of key governance bodies*

There may be a need to clarify the roles of the Executive committee and the Strategic Direction committee. The coordinator should consider taking a more active role in the Executive committee. Ways to improve communication about the issues discussed and decisions taken at these boards to all partners should be explored.

### *5.2.2 Enhance internal communication*

Further efforts should be made in strengthening communication and interactions between the transversal and technical WPs. Focus should be more on contents than on tools.

### *5.2.3 Enhance outreach and external communication*

SPARTA should explore ways to further strengthen collaboration with the other 4 pilots to ensure that the relevant experiences and messages are communicated to the planning and setting-up the ECCCN.

SPARTA should pay more attention to clearly informing partners, associates, and friends of how they can contribute, when, and where they can see the impact of their contributions. Publishing summaries of the collected feedback and indicating how it will be used and has been used to shape SPARTA activities should be considered.

National SPARTA events have been received positively. SPARTA should experiment more with thematic events fostering cross-border participation. This can help gain experiences relevant for the ECCCN, which will also manage both national (NCCCs) and European (ECCC) events.

### *5.2.4 Ensure learning from SPARTA experiences*

SPARTA should consider working together with the other pilots in preparing a joint policy brief highlighting the relevant experience from all 4 pilots. The policy brief should raise and discuss all relevant issues that need to be addressed in the context of ECCCN, including controversial ones.

Since SPARTA is planned to end one year earlier than some of the other pilots, there is a danger that SPARTA experiences will have a more limited impact in the design of ECCCN structures and activities. This may also result in a gap between the ending of SPARTA activities and the launch and establishment of the new activities of the ECCC and the NCCCs and thereby a loss of momentum gained in SPARTA as well as loss of tools, assets and networks developed in SPARTA. SPARTA should therefore consider proposing a limited continuation to SPARTA to ensure dissemination, exploitation, and transfer of SPARTA experience to ECCCN. This could take the form of a **Horizon Result Booster project**, which is meant for disseminating project results.

### *5.2.5 Strengthen SPARTA as a proper governance pilot*

There have been obvious limitations for SPARTA to act as a proper pilot towards the ECCCN, mainly related to operating under the Horizon 2020 project administrative context, the lack of dedicated budget allocation to launch new research activities and operating during the COVID-19 pandemic travel and meeting restrictions. To overcome these limitations, SPARTA should consider deliberate measures to gain further experience as a proper governance pilot.

What this means in practice is e.g., making changes to the work plans of the technical WPs based on changes made to the roadmap. While there have undoubtedly been valid reasons not to change these work plans, continuing without any changes will eventually limit SPARTA as a proper governance pilot.

It would be important that SPARTA gains at least some experiences in managing an adaptive portfolio of research projects. One possibility would be to add new projects to the portfolio, but this is not possible as SPARTA budget does not foresee this. Another possibility would be to redirect funds from less important projects to other more important projects or new projects. As this has not been done one can only assume that SPARTA research portfolio has no less important projects.

The third way to experiment with an adaptive research portfolio is to identify synergies between research projects and redirect them so that these synergies can be better captured. While this is the least invasive approach and thereby also most limited in terms of gaining relevant experiences, it might be the most appropriate for SPARTA in the given context. This will require systematic identification and analysis of synergies and the potential benefits in capturing them. Report D.1.2 lists several potential areas where synergies may be found.

Ideal situation would allow experimentation with the "fail often, fail fast" approach, e.g., by launching an open call for new research ideas, selecting several ideas and funding them for a 3 or 6-month initial exploratory stage, and then letting only the most promising one or ones to continue as a full-scale research project. The same approach could also be experimented with within planned projects, e.g., by asking several parallel teams to work on a task and then after a while selecting the most promising one to complete the task. However, this would require that a project has the sufficient resources to allow for some levels of effort duplication, which is not normally the case.

Eventually, the ECCCN will operate as a network with highly unbalanced actors as some of the NCCCs will have much bigger resources and stronger national networks and actors than others. This may result simply from the differences in size, but also from prioritisation of cybersecurity in the overall policy agenda, and differences in international collaboration interests (e.g., towards NATO or global open-source communities). SPARTA is a good environment to collect relevant experiences from governing a network which has both stronger and weaker national nodes. Collecting and analysing these experiences systematically is the fourth way SPARTA could strengthen itself as a pilot during the remainder of the project.

## 5.3 Observations related to the ECCCN

Before discussing the observations related to adopting SPARTA experiences in the coming ECCCN context it should be noted that the roles and mandates of the ECCC and the NCCCs have not yet been fully fixed. It is also unclear what the role of ECSO and other existing networks and platforms in the European cybersecurity community will have in the future. This should be kept in mind while considering the observations presented below.

### *5.3.1 Governance principles*

The governance principles of SPARTA are very well aligned with the principles defined for European partnerships. As the new ECCCN structure is seen at least partly as a European partnership, learning from experiences with the governance principles of SPARTA is relevant. Based on the assessment, three governance principles are of particular interest in this respect: openness and transparency, flexibility and risks, and diversity.

#### 5.3.1.1 Openness and transparency

Openness and transparency are controversial issues in the context of cybersecurity. One approach emphasises that ensure security is about closing doors and limiting access. Completely opposite approach is to bring everything into the open, and thereby using the wisdom of the crowd to identify potential security related issues and problems. The diversity and the scales of grey between these extremes means that there cannot be a single simple approach to adopting the principle of openness and transparency in the ECCCN context.

However, there are several areas of governance where the principle of openness and transparency can be universally adopted. These are specifically related to decision making and directionality of common European action. The need for increased openness and transparency has been identified in the 2017 evaluations of both Art. 187 and Art. 185 partnerships[42,43].

SPARTA experience indicates that there are significant benefits from establishing transparent processes for identifying, raising, discussing, and eventually making decisions about shared concerns and common issues. The same applies to stakeholder consultations, where it is important to openly communicate the collected views either as such or in anonymous aggregates, as well as indicate where, how, and when these views will be used e.g., for making important decisions. This is a principle that can be adopted both by the ECCC and the NCCCs, and any community network managing relevant governance processes such as roadmap work.

While openness and transparency may be adopted as a general principle, there might be a need to make exceptions to it in specific cases. These might be related to e.g., specific cybersecurity threats and how these can be prevented, limited, and managed, or specific promising new technologies with high commercial value.

Openness and transparency regarding new technological developments, research and its results, new tools and applications, etc. is a more controversial issue. While there may be clear benefits from openness and transparency e.g., in supporting increased cybersecurity awareness, reducing duplicate efforts, etc., there are also viable reasons for keeping some of these behind closed doors, e.g., for commercial and security reasons.

The ECCC should promote openness and transparency and work in collaboration with actors promoting open access to establish open platforms, resources, tools, and applications. The primary purpose of this would be to support increased cybersecurity awareness among people and companies in Europe. This would be based partly on voluntary action of interested likeminded actors, and partly on commissioning the development and deployment of platforms facilitating access to and use of shared tools, applications, technologies, etc.

The NCCCs could consider a similar approach in a more limited national context, especially if smaller communities of cybersecurity practitioners can be identified who could particularly benefit from mutual exchange of technologies, tools, applications, etc. These communities of practitioners could also extend cross-border in collaborations between NCCCs and possibly also with relevant European institutions.

However, it is important to note that while openness and transparency is a good governance principle and can provide significant benefits, it cannot be adopted as a universal approach in the ECCCN context. There are areas of governance especially related to critical assets where openness and transparency must remain limited.

#### 5.3.1.2 Flexibility and risks

While the SPARTA and other earlier experiences clearly indicate that a well-planned and expertly prepared research agenda or roadmap can provide a good and solid basis for longer-term research, cybersecurity is an area where new threats emerge frequently. This means that even the most excellent roadmap will soon become outdated and needs to be updated.

---

[42] Meta-Evaluation of Article 185 Initiatives, Report of the Expert Group, DG Research and Innovation, 2017 (https://www.era-learn.eu/documents/a185_meta_evaluation_expert_group_report-1.pdf)

[43] Mid-term review of the contractual Public Private Partnerships (cPPPs) under Horizon 2020, Report of the Independent Expert Group, DG Research and Innovation, 2017 (https://op.europa.eu/en/publication-detail/-/publication/6de81abe-a71c-11e7-837e-01aa75ed71a1)

While the SPARTA approach of periodically updating the roadmap may not be unique, it certainly confirms that such a process is important for any network pursuing common actions.

What the SPARTA experience is more limited in is how to introduce and implement sufficient degrees of flexibility and adaptability into the common action based on the identified changes in the cybersecurity environment. However, the lack of SPARTA experience due to implementing it in the Horizon 2020 project administrative context does not mean that this is not an important characteristic of the ECCCN.

The ECCC and the NCCCs at the national level and as a network should consider adopting the principle of flexibility and adaptability. Since the ECCCN structure is identified partly as a European partnership, this is mandatory anyway.

However, what is not necessarily mandated by the EU partnership principles is the more positive attitude towards risks, e.g., the fail-often-fail-fast approach. While SPARTA may not have much experience from operationalising this principle, it is positively viewed in the SPARTA network.

The ECCC and the NCCCs should consider call and funding modalities which are more acceptable towards risks and changes in the project portfolio. This means not applying the Horizon 2020 type restrictive and highly pre-defined modality of funding projects, but instead more open approaches to selecting, ending, merging, and implementing projects in stages. One possible approach is to launch open calls to select a larger number of projects to test their feasibility and after 6 months or a year, reduce the number of projects by ending, merging, and redirecting some of them to arrive at a portfolio of projects optimally aligned with the roadmap of the call. The same exercise may then be repeated e.g., after another 1.5 or 2 years, when also new projects could be added to the portfolio. This approach could be complemented by leaving parts of the budget to be allocated later when new highly relevant issues emerge and are added to the roadmap, or if none are identified, the funds can be used for strengthening existing highly relevant projects in need of additional resources.

Clearly not all research can or should be implemented using more flexible approaches to managing portfolios of strategic research based on a roadmap as described above. The modalities used in allocating funds under the Horizon Europe will likely remain close to the modalities currently used for Horizon 2020 projects. While national funding may utilise more flexible funding modalities, these will most likely largely follow the existing national practices. The most relevant actor in the ECCCN landscape for promoting a more flexible and adaptive approach combined with the fail-often-fail-fast ideology, and thereby developing and using new modalities is the ECCC and especially how it develops modalities for designing, launching, and managing portfolios of strategic cybersecurity research.

#### 5.3.1.3 Diversity

Like discussed under openness and transparency, there are contradictory views in the wider cybersecurity community on various issues. Further diversities can be found in the cultural and geographical contexts (e.g., formal vs. informal, levels of trust, societal priorities, etc.), people and their personal values (e.g., gender, religion, etc.), as well as research and applications domains (e.g., social sciences, ICT, security, defence, civilian, business, etc.).

The approach of SPARTA is to use diversity as a strength rather than see it as a problem. The assessment indicates that SPARTA has been able to capture benefits originating from actively promoting and making use of diversity.

One area where the ECCC, the NCCCs, and the Community may benefit from SPARTA experience is in promoting interaction and discussion about controversial and highly important issues, such as openness and transparency, approaches and measures available for developing European strategic autonomy or supply-chain resilience in the global context, or how to increase awareness and reduce cybersecurity risks among European citizens. Enabling and facilitating lively interaction on important cybersecurity issues including the more

controversial ones, is an important activity and shared responsibility of all actors in the ECCCN landscape.

Besides discussion, especially the ECCC and to the extent appropriate the NCCCs should promote the design, launch, and implementation of cross-disciplinary, cross-border, cross-industry, etc. collaborative efforts. All countries, industries, people, etc. do not face cybersecurity threats equally. Some actors must make more efforts in preventing and preparing for them. It is important that efforts are made to facilitate fast transfer and learning from the experiences of the more advanced cybersecurity actors to keep the rest better prepared for future threats. The role of the ECCC is particularly relevant here as the Community and to some extent the NCCCs tend to organise into networks and consortia of likeminded actors, e.g., similar industries, approaches, methods, and tools, similar demographics and geographies, similar cultures, etc.

The ECCC's role here may be even more important for two additional reasons. First, it may be a key actor in the interaction between Europe and other global regions and actors. Second, it has a specific role to coordinate across NCCCs, which reflect their respective national cultural, societal, and policy priorities. The ECCC may therefore have a specific role together with the Commission to define the European way to manage e.g., the balancing act between increasing protection against cybersecurity threats and at the same protecting access and use of personal data. Developing mobile tracking applications for COVID-19 compliant with the needs and GDPR has been an interesting case. It shares many of the same features as the highly relevant issues in cybersecurity, such as balancing the needs for surveillance and identification to capture those behind cybersecurity threats, and the GDPR and other regulations ensuring privacy and protection of personal data.

### *5.3.2 Governance tools*

The observations from the assessment indicate that some of the approaches and tools adopted or developed in SPARTA may be relevant for the ECCC and the NCCCs, possibly also to the Community. These include the roadmap work, self-assessment tools, and governance audits.

#### 5.3.2.1 Roadmap work

According to the assessment, the SPARTA roadmap work is of high quality. The key learning points related to it are:

- The roadmap work should be driven and managed by high level experts, including sufficient methodological expertise
- The roadmap should be regularly updated
- The roadmap work should invite wide participation from the Community
- The roadmap work should be linked to forward-looking activities such as horizon scanning and other types of foresight

With these learning points, the SPARTA experience clearly confirms the validity of the recommendations related to roadmap work given in the Mid-term review of the contractual Public Private Partnerships (cPPPs) under Horizon 2020[44], i.e., the need to include all

[44] Mid-term review of the contractual Public Private Partnerships (cPPPs) under Horizon 2020, Report of the Independent Expert Group, DG Research and Innovation, 2017 (https://op.europa.eu/en/publication-detail/-/publication/6de81abe-a71c-11e7-837e-01aa75ed71a1)

stakeholders into the roadmap work, and that the roadmap must be maintained current by updating it periodically.

SPARTA roadmap is one roadmap among many as the other pilots have their own roadmaps, ECSO has its own, many actors have their own, and the Commission has their own Horizon work programmes.

There will inevitably be several active roadmaps also in the future ECCCN landscape. The ECCC and all the NCCCs must each prepare their own roadmaps, and the Community will probably have several prepared by the different networks active in the wider community. Some of these will be more oriented towards scientific research, some more towards technological developments, some focused on specific industries or application areas, etc.

What is relevant in this context is especially how the roadmap for the ECCC is prepared and how sufficient alignment between it and the roadmaps of the NCCCs is ensured. This will require a periodically updating roadmap process to be established in collaboration between the ECCC and the NCCCs. Furthermore, this process will have to include ways to ensure participation of the wider cybersecurity community either directly (collection of views directly from all actors e.g., in the Atlas), or indirectly (collection of aggregated views from the different sub-communities and networks active in the wider European cybersecurity community), or both using a combination of direct and indirect methods.

It may be that ECCC will eventually prepare more than one roadmap, perhaps one focusing more on scientific research, and other more on technologies, applications, and/or industries. Regardless of eventually ending up with one or many ECCC roadmaps, the roadmap process should be managed by the ECCC. The ECCC may want to use existing expert body or bodies to manage the process(es) or establish separate one(s). The ECCC roadmap work should be supported by an on-line tool for data collection, as well as method and tools for sense-making. There should also be a clear and transparent process how the new observations from the roadmap work lead into roadmap changes, and how these changes will be reflected into the work plans of projects in the ECCC strategic research portfolios, and the reorientation and composition of the ECCC strategic research portfolios.

Another SPARTA learning point is to put sufficient emphasis on transparency, i.e., publish views or aggregates of them, while clearly indicating for what purposes, how, and when they will be used. Seeing the impact of earlier contributions is likely to increase motivation to contribute later.

#### 5.3.2.2 Self-assessment

Increasing awareness of European citizen and companies about cybersecurity threats and how to prepare for them is a continuous task. The more aware and prepared the people and organisations are, the less likely these threats are to materialise and cause problems.

One of the positive experiences from the SPARTA associates and friends -network is from the use of a self-assessment tool developed in SPARTA for assessing the awareness and knowledge of cybersecurity among an organisation's staff. This can be used as a basis for developing targeted staff trainings. Widely usable tools and applications such as this one used in SPARTA can be very valuable in raising awareness and helping to identify training needs.

The ECCC should together with the NCCCs explore the possibility and viability of adopting, developing, commissioning, or otherwise making available such tools, which will allow citizens and employees as well as companies, and other organisations to raise cybersecurity awareness and identify and develop targeted trainings for key people and organisations.

A possible area for systematic collaborative action between ECCC and the NCCCs could be e.g., implementing awareness and training campaign targeted to organisations and their staff managing critical European and national infrastructures.

#### 5.3.2.3 Audits

According to SPARTA experience, it is important to remind people of the underlying principles. One possible approach is to use periodical governance audits. Adoption of principles can be monitored in the context of a wider governance or financial audit, or it can be subject to a dedicated audit. Besides acting as a reminder and thereby ensuring adoption, an audit may reveal needs to clarify or further develop the interpretation of the principles.

### *5.3.3 Network management and stakeholder interaction*

SPARTA experience in managing community networks and external stakeholders may also be relevant for both the ECCC and the NCCCs. The most important aspects in this respect are the tiers-of-trust approach, proactive interaction, and brokerage between users and researchers.

#### 5.3.3.1 Tiers of trust

SPARTA has a core consisting of 44 partners of which 13 lead specific WPs. Partners are bound together through legal contracts related to the implementation of SPARTA project. Around the core of partners, SPARTA has invited additional organisations with similar interests. These are associates and friends. Specific processes and practices have been established for interacting with the associates and friends.

The learning point here is that this approach – partners, associates, friends, outside world – is appreciated by the associates and friends. A similar approach could be viable also in the ECCCN landscape.

However, the ECCCN landscape is more complex in this respect. First, the NCCCs will each have to develop their own national network. It is not clear if all NCCCs will follow a common set of criteria or develop their own. Second, it is not clear if the approval of the local NCCC will be automatically accepted at the European level (presumably ECCC controls approval and access to the Atlas). Nor is it clear if there is a separate European approval and if that may be automatically accepted by the NCCCs. Third, establishing relations to non-national and non-European actors is important, but it is not obvious how it may be systematically coordinated across the ECCCN. Hence, it is difficult to see if it is even possible to establish a similar tiers-of-trust network structure in Europe. Tiers-of-trust may be a possible approach at the national level. However, it may also not be possible because of political reasons.

It is likely that the tiers-of-trust approach may be most relevant at the level of specific initiatives, and possibly in the context of the ECCC and the NCCCs as far as it may be applied to community networks, platforms, associations, etc. The ECCC and/or the NCCCs may invite and approve a more limited number of key networks, associations, and other groups of cybersecurity actors to collaborate inside a closer tier-of-trust. This may be applied to specific sections of the wider cybersecurity community, such as defence, police, critical infra, etc.

Regardless of where the tiers-of-trust approach is used and whether it is used by specifically referring to trust or simply to levels of engagement in a more general sense, it is important that the criteria used for approving actors to specific levels are transparent, same as the possible additional benefits of being accepted to the higher tiers-of-trust.

In any case, tiers-of-trust is a viable approach to optimise interactions with the community in cases where there are legitimate reasons to differentiate between external stakeholders.

#### 5.3.3.2 Proactive approach

SPARTA experience indicates that proactive interaction is valued by external stakeholders. Rather than relying on making information available, the ECCC and the NCCCs should reserve sufficient resources and establish appropriate processes to enable and encourage proactive interaction with external stakeholders.

#### 5.3.3.3 Brokerage events

Associates and friends of SPARTA value the Associates Council, but especially the Brokerage events. The main feature of these events is that they bring together users, companies and researchers around specific user cases and technological opportunities. As such, they take the interaction at a very practical levels of application. This has proven a good approach for identifying who else has similar challenges and how potential solutions could be developed. This is also a good basis for identifying partners and ideas for future collaborative projects.

Both the ECCC and the NCCCs can learn from this SPARTA experience, which is very much aligned with the mission-oriented approach planned to be adopted in Horizon Europe, and recommendations presented in earlier partnership evaluations calling for more focus on outcomes and impacts[45], and moving towards a mission-driven approach[46].

### *5.3.4 From the four pilots towards the ECCCN*

Moving forward from the four pilots to the ECCCN does not represent a traditional transition or handover from one established structure to another. However, there are some similarities, particularly related to assets developed in the pilots. These assets may be tangible such as tools, applications, technologies, etc., or they be intangible such as networks, tiers-of-trust, etc.

SPARTA experience also refers to issues that need to receive more attention in future when planning to launch similar pilot projects.

#### 5.3.4.1 Pilot actions

As indicated in earlier sections of this report, SPARTA is being implemented in a context that does not allow it to act as a proper governance pilot for the ECCCN. SPARTA has not been able to experiment with the levels of flexibility needed from the ECCCN and especially ECCC. Furthermore, it has not been able to gain experience from managing calls, launching new research, and managing a dynamic strategic research portfolio.

The experience from SPARTA as a governance pilot implemented in a less-than-optimal context with less-than-optimal flexibility and resources suggests that before launching future pilots for similar purposes a number of issues should be considered.

First, similar pilots should be launched under much more flexible modalities to allow real piloting. The Horizon 2020/Europe project administrative context to too rigid for piloting. For example, similar governance pilots should be allowed a dedicated budget allocation for yet undefined future activities, which would make it possible to experiment with a much more dynamic strategic research portfolio. Similarly, they should experiment with stage-gate approaches for selecting and funding projects, as well as ending, merging, and scaling up projects. Pilots could also have additional resources to deliberately launch duplicate efforts for a limited time to see which alternatives prove more effective and efficient.

Second, should future piloting consist of several parallel pilot projects, synergies should be captured through complementarities and collaboration as soon as the original selection is made. It is not clear why the competitive environment between the pilots was maintained for more than a year after the four pilots were originally selected.

Third, to ensure that all relevant experiences from all pilots are transferred as learning points to the design, launch and activities of the ECCCN, a dedicated taskforce to advice in the remaining planning and launching of the key ECCCN activities is proposed. The taskforce

[45] Meta-Evaluation of Article 185 Initiatives, Report of the Expert Group, DG Research and Innovation, 2017 (https://www.era-learn.eu/documents/a185_meta_evaluation_expert_group_report-1.pdf)

[46] Mid-term review of the contractual Public Private Partnerships (cPPPs) under Horizon 2020, Report of the Independent Expert Group, DG Research and Innovation, 2017 (https://op.europa.eu/en/publication-detail/-/publication/6de81abe-a71c-11e7-837e-01aa75ed71a1)

should have members from the four pilots, ECSO, and the ECCC and Commission, and selected representatives from Member states. Such a taskforce can be useful especially in transferring experiences that are difficult to describe explicitly (intangibles). To manage the transfer of experience, the taskforce should continue until all the key activities of the ECCC and the network of NCCCs have been launched.

#### 5.3.4.2 Assets

Some of the SPARTA associates and friends are concerned that the services they now can access because of SPARTA and the momentum they have been able to build with the help of SPARTA may disappear after SPARTA as a project end.

It is important to find ways to ensure that relevant assets developed in SPARTA and the other pilots are assessed and most relevant ones continue to be developed in the ECCCN. One of these assets is the JCCI repository, and the self-assessment tools developed in SPARTA. Another one is the SPARTA associates and friends -network.

Observations have been made above and earlier in this report with respect to ensuring SPARTA involvement during the transition from the four pilots towards the ECCCN. In addition to those facilitating observations, more specific processes, assessment criteria, etc. should be developed to support a systematic assessment of the assets developed in the four pilots. Furthermore, the relevant assets found in the systematic assessment should be integrated to the relevant ECCC activities and more detailed action plans describing how they will be developed and launched.

#### 5.3.4.3 Community support

As indicated earlier, it is not clear how the wider cybersecurity community is planned to be organised or plans to organise itself beyond merely collecting all interested and credible actors into one single Atlas. There are indications that ECSO may continue, but it is not clear whether it will continue to enjoy a similar special relationship to the Commission as it now has.

The NCCCs may simply rely on sufficient interest among all cybersecurity actors to get accepted and thereby ensuring that they are eligible for future funding. How each NCCC will eventually interact with different sub-communities nationally is for them to decide. Depending on the quality and volumes of human and funding resources available, the NCCC may develop tailored approaches to different sub-communities in addition with specific cross-community action and generic action targeting all.

The real challenge is at the European level, where the ECCC needs to find a suitable balance between interacting with the network of NCCCs and the wider cybersecurity community and its various sub-communities. The key decision the ECCC and the Commission will have to make in this respect is whether they foresee the need and added value in any action targeted for supporting networking within the wider cybersecurity community at the European level.

The support could be based on the tiers-of-trust approach by identifying the most relevant sub-community representatives and giving them a special position. The special position could be in general or it could be more limited to specific actions, like roadmap work.

If stronger support is foreseen, this could take the form of an open call offering funding for the coordination of specific types of cybersecurity networks or networks in general. This could be modelled along the lines of similar funding support made available for similar purposes at the European level.

#### 5.3.4.4 Policy alignment

SPARTA has extensive experience in identifying and understanding the different policy needs and trends as well as different approaches to cybersecurity related challenges from its roadmap work, collaboration with the other 4 pilots, work with associates and friends, including national authorities, and more recent work aimed at global actors outside Europe.

These experiences may prove valuable especially in view of developing the future activities of the ECCC aimed at identifying, understanding, and capturing potential synergies with other European and international initiatives. The ability of the ECCC and the ECCCN to create added value and impact beyond the funded projects may depend largely on its ability to capitalise on the potential synergies.

Identifying synergies with Digital Europe and Horizon Europe should be obvious as they form the wider European policy context for the ECCCN. However, ECCC and the NCCCs should not be limited to these as understanding what happens globally and in other policy areas might help identify relevant future cybersecurity issues and allow early detection and capture of potential synergies. Identifying and capturing synergies with relevant national, European, and international initiatives has also been identified as a recommendation in earlier partnership evaluations, particularly regarding public-public-partnerships[47], which is what the partnership nature of the ECCCN primarily is.

### *5.3.5 Monitoring and evaluation*

#### 5.3.5.1 Measurement

Monitoring the impact of cybersecurity research and innovation activities is more challenging than in many other sectors. This is because in many cases the eventual big impact that should be measured is cybersecurity threats and events prevented. Measuring the absence of something and the value of it can only be done in a clearly defined context, especially since the objective cannot be total prevention as that would not be realistic.

This means that relevant KPI must be partly based on a realistic counterfactual, which may be an international comparative. One possible counterfactual could be built on risk management, i.e., identifying and assessing the probability and impact of risks related to possible cybersecurity events, and assessing occurred real events and their impacts against the risk assessment. Other possibilities may be changes in numbers of cases over time or estimates of losses cause by breaches. However, making these really viable would also require international comparison.

The analysis of SPARTA KPI clearly indicates that to facilitate the monitoring of impacts of awareness, training, and other competence related activities, it would make sense to develop and adopt models for identifying different levels of personal awareness, personal competences, organisational awareness, organisational preparedness, organisational competences, etc. These models could then be used as a basis for developing and offering web-based self-assessment tools and collecting and using data for monitoring the impacts of related measures.

Another important monitoring systems development aspect is to define KPIs that indicate the contribution and added value of specific activities on the outcomes and impacts. Otherwise, it is not clear what the role of the monitored activities has been on the outcomes and impacts, which makes it impossible to assess if the resources allocated and used for the activities have been necessary or used effectively and efficiently.

#### 5.3.5.2 Approach

Designing a monitoring and evaluation system for the ECCC, the NCCCs and for the ECCCN should be compliant with several requirements. Depending on the sources of the eventual budget allocations for ECCC and NCCCs, the monitoring and evaluation system must comply with the relevant European and national regulations, most likely with Horizon Europe funding regulations, relevant state aid regulations, as well as regulations concerning the use of national

[47] Meta-Evaluation of Article 185 Initiatives, Report of the Expert Group, DG Research and Innovation, 2017 (https://www.era-learn.eu/documents/a185_meta_evaluation_expert_group_report-1.pdf)

public funds. Furthermore, the monitoring and evaluation system must comply with the needs to measure the impact of relevant policies. At the European level this refers to policies such as the Digital Europe, and at the national level all policies with sufficient emphasis on digitalisation and security.

Furthermore, the monitoring and evaluation system will inevitably consist of several layers. The most detailed levels of monitoring are most likely the individual projects and the individual actors. While project monitoring will most likely largely follow existing European and national practices, monitoring of actors will most likely be based on separately organised efforts, such as ad-hoc or periodical surveys. The more aggregated levels of monitoring and evaluation are the initiatives such as collaborative programmes, and the various cybersecurity networks and sub-communities.

Monitoring of the initiatives will be largely based on aggregate data collected from projects funded and implemented under the initiative. However, to measure the added value of the initiatives beyond the aggregate of its projects, an additional layer of monitoring must be established. This may be introduced as a requirement to the actors selected to manage the initiatives. Monitoring of the networks and sub-communities presents a specific challenge as it may not be built on any aggregates. A separate approach is therefore needed. One possibility is e.g., to establishing an observatory[48] for monitoring the developments of e.g., awareness and competences of actors or groups of actors, or monitoring the developments of community networks and sub-communities e.g., through changes in participations and types of engagements over time. Posing the monitoring and reporting requirement to the actors managing these networks and sub-communities could also be an option, but that will most likely require some form of financial support to them.

The top level in the monitoring and evaluation system is the performance and impact of the whole ECCCN network. This is a rather complex task. The monitoring system will most likely rely largely on the aggregation of the monitoring data from the more detailed levels, i.e., from projects and initiatives. However, the ECCC and the NCCCs will have to establish further systems to measure three dimensions in particular, the added value of the ECCCN, the impacts among the actors, community networks and sub-communities, and impact of activities beyond projects and initiatives.

While many of the monitoring requirements can be met using data collected from funded projects and initiatives, additional data collection must be organised for the rest. To ensure sufficient consistency and cross-use across the ECCC and the NCCCs, the monitoring and evaluation system should be designed in collaboration.

It is obvious that the ECCCN level evaluation and possibly also part of its monitoring must be sufficiently independent. However, using external independent assessment also at the more detailed levels of the ECCCN could be considered. This is where the SPARTA experience may prove useful. This report illustrates the use of external assessment of SPARTA governance and especially how it may support the development of the ECCCN governance as a pilot. A related issue is to use external assessment for a similar purpose in other pilots preceding the design of a new European structure.

The experiences from this work indicate that an external assessment can be quite useful in identifying aspects which might be more difficult to see from the inside. External assessment may also raise questions, which may be related to yet unvoiced underlying concerns. While this assessment has not revealed previously totally unidentified issues, it has been able to draw attention to issues relevant for the implementation of SPARTA as a pilot supporting the design

[48] European observatories that could be used as a model include e.g., https://clustercollaboration.eu/tags/european-cluster-observatory, https://www.eublockchainforum.eu/, or https://www.hspm.org/mainpage.aspx

and launch of the ECCCN even better. Furthermore, the assessment has clearly indicated areas of SPARTA experience highly relevant for the ECCCN.

Similar external assessment could therefore easily be considered for similar pilots in the future with the aim to support the development of a new European structure. The experience may also be relevant in view of the need to monitor and evaluate the ECCC and possibly the network of NCCCs. An independent external assessment may also be appropriate because of the underlying set up of the ECCCN effectively as a partnership between the EU Commission, Member states, and its networking with the European (and international) cybersecurity community.

The approach chosen here focusing on effectiveness, efficiency, coherence and eventually relevance, is highly valid for any similar independent external assessment of pilots. The same approach may also be viable for any possible pilot action initiated by the ECCC or the NCCCs towards engaging sub-communities or supporting the self-organisation within the community. The purpose of these pilots is to see whether the actions piloted are relevant for the ECCCN and thereby worth exploring further or launching in larger scale.

However, the approach used in this assessment should be adopted when used for monitoring and evaluation purposes. The relevance in normal monitoring and evaluation purposes takes a different meaning, i.e., how relevant is the measured effort in view of the objectives of the monitored or evaluated action. The fundamental meaning of effectiveness, efficiency and coherence remains unchanged, but will naturally have to be adopted to the specific context of the monitored or evaluated action.

The main challenges in using independent external assessments are typically related to access to data and available resources. The former may limit the external assessment to selected parts of governance, which may lead to missing issues or misinterpretations, and eventually less relevant or even wrong conclusions and recommendations. The latter may have similar consequences, especially if data collection and interactions are very biased, and methodological approach is limited.

In view of the ECCC and the ECCCN, one of the major challenges during the launch and winding-up period is to design, establish, and consolidate an effective and efficient governance model with appropriate principles, structures, processes, etc. An independent external assessment such as this implemented in SPARTA could potentially prove quite useful once the governance model has been designed and established, but not yet fully consolidated.

# Appendix A Analysis of SPARTA key performance indicators

*Table A1 Relevance of SPARTA KPI for the pilot and the future ECCCN*

| **SPARTA objective** | **SPARTA KPI** | **Relevance of the KPI[49]** | | |
|---|---|---|---|---|
| | | the pilot | ECCCN | Comments |
| 1. Create a networked governance for advanced cybersecurity research in Europe | #1.1 – Governance structure and decision-making mechanisms defined and implemented before M4 of the project | x/o | x/o | This is not a relevant KPI for the pilot or the ECCCN, but rather an early milestone of the project. |
| | #1.2 - # of issues about the governance escalated to the General Assembly | x/c | | Little relevance as a KPI for the pilot and not relevant for the ECCCN. This can be used as a monitoring indicator at the beginning of a new initiative to indicate how fast and when the governance system becomes established. However, as the baseline and relevant objectives can be set only after the initiative is launched and it is seen how many issues are raised at the beginning when the governance system is yet to be fully established, this cannot be set a-priori and therefore it is not viable as a KPI. This could be used as a temporary KPI during a launch stage or after significant governance system changes, but even then, this should refer only to unnecessary issues, since some issues are planned to be raised even when the governance system is fully established and optimised. |
| | #1.3 – Level of satisfaction of the network members (survey – 1 – 7 Likert scale) | xx/p | xx/p | A viable and moderately relevant KPI indicating participant satisfaction. This should preferably be a composite indicator consisting of participant satisfaction into all key aspects of governance, or whatever is the measured activity. This approach is more suitable for measuring changes in satisfaction than absolute level of satisfaction. |
| 2. Define and sustain an EU-wide roadmap at the cutting-edge of cybersecurity research and innovation | #2.1 - Quality and sustainability of the roadmap: number of surveys, number of contributors, number of revisions and feedback received, mappings with other initiatives, etc. | xxx/p | xxx/p | It should be evident that all or at least most calls would be aligned with the ECCCN roadmap(s), hence using this as a KPI is not relevant. In fact, it might be even more relevant to consider having a specific objective to deliberately explore new avenues of research outside the main calls and use that as an indicator instead. |
| | #2.2 - # of calls (national and EU) aligned with SPARTA Roadmap | xxx/p | x | It should be evident that all or at least most calls would be aligned with the ECCCN roadmap(s), so using this as a KPI is not relevant. In fact, it might be even more relevant to consider having a specific objective to deliberately explore new avenues of research outside the main calls and use that as an indicator instead. |
| | #2.3 - # and amount of funded projects (national and EU) aligned with the SPARTA Roadmap. | | | |

[49] Relevance is xxx = high, xx = moderate, x =low; measurement should be done o = once, p = periodically, c = continuously

| | | | | |
|---|---|---|---|---|
| 3. Build sustained collaborations with academic, industrial, governmental, and community stakeholders | #3.1 - # of SPARTA workshops organized and # of attendees per workshop | xx/p | xx/p | Measuring participation into workshops, or better yet numbers of first-time participants can be useful for understanding the role workshops play in raising awareness and expanding the community. Numbers of workshops organised is much less relevant as a KPI. |
| | #3.2 - # of collaborations: liaisons with national and EU projects, and other projects | xxx/p | xxx/p | This is relevant, but must be redesigned for the ECCCN context, e.g., by focusing on the alignment and collaboration between activities launched by the ECCC, the NCCCs, and under the Horizon Europe calls. |
| | #3.3 - Share of women in groups and workshops | xxx/p | xxx/p | This should be complemented with other indicators equally relevant indicators indicating progress towards equality and diversity. |
| 4. Innovate to address transformative strategic challenges | #4.1 - Ranking and # of publications | xx/p | xx/p | Relevant in indicating the impact of research activities, but less relevant for indicating impact of the governance pilot. |
| | #4.2 - # of research results co-authored by both SSH and computer scientists | xxx/p | xxx/p | Like the KPI 3.3, this should also be developed further so that it can better indicate different types of diversities and synergies and impacts materialised by capturing them. |
| | #4.3 - # of technological assets produced in SPARTA programs | xx/p | xx/p | Indicates outcomes, which are important to measure. However, this must be developed further to better indicate different types of assets and their value for the Community and in view of relevant European policy objectives (e.g., European strategic autonomy). |
| 5. Support cybersecurity design, testing, evaluation, and certification capabilities | #5.1 - # of certification requirements covered by SPARTA technologies | xxx/p | xxx/p | Certification is highly relevant as such, but to what extent this is a relevant KPI depends eventually on the specific role, mandate and activities of ECCCN. |
| | #5.2 - # of technologies used in the labs | x | x | The number of technologies may indicate very little, until it is assessed in a relevant context against a pre-defined objective. To what extent this may be a relevant KPI depends eventually on the specific role, mandate and activities of ECCCN. If ECCCN or ECCC or NCCCs aim to develop and maintain a catalogue or even a repository of technologies, this may be highly relevant. |
| | #5.3 - # of platforms and access policies formally identified | x-xxx/c | x-xxx/c | It is highly relevant that the ECCCN has a continuously updated index and key information of the available platforms, access policies, and interoperability and possible joint usage of labs. This may also be relevant as a KPI if there are specific objectives to increase these. Otherwise, these are less relevant as KPIs. |
| | #5.4 - Interoperability and possible joint usage of the labs | | | |
| 6. Enhance awareness and training capabilities and develop | #6.1 - # of courses executed using the curricula developed by the project | xxx/p | x-xxx/p | This is highly relevant KPI for the pilot. Relevance for the ECCCN depends on future roles, mandates and activities of the ECCC, the NCCCs and the Community, respectively, especially on whether there are specific efforts in developing and maintaining shared European curricula. Trainee satisfaction is more relevant than the number of courses |
| | #6.2 - Satisfaction and # of trainees who successfully finished security- | | | |

| | | | | |
|---|---|---|---|---|
| cybersecurity skills | related courses designed within the project | | | |
| | #6.3 - # of directly addressed people (through participation at conferences, workshops, trainings, etc.) by the awareness program by the end of the project | x-xx/o | x-xx/p | Measuring the impact of awareness and outreach activities is important. However, the real impact of outreach is in the increased awareness and eventually behavioural change in the people and organisations reached by the activities. Participations may be used as crude proxies as they may already indicate some levels of awareness, but there is no evidence to suggest that they are reliable proxies for impact. |
| | #6.4 - # of indirectly addressed people (through advertisements, social media groups) by the awareness program by the end of the project | | | |
| 7. Demonstrate ethical sustainability | #7.1 - # of SPARTA results licenced | xx/p | xx/p | Relevant for the pilot to indicate that the research addresses real needs of companies, and indirectly, the quality of the roadmap. Similarly, relevant for the ECCCN, but more challenging to operationalise across ECCC, the NCCCs, and Horizon Europe. |
| | #7.2 - # of patents produced, software components registered or open-sourced | | | |
| | #7.3 - # of start-ups created over technological assets produced in SPARTA | | | |
| | #7.4 - # of responsible research and innovation debates and # of participants | x-xx/p | x-xx/p | Little relevance as a generic indicator. Could be more relevant if defined as an indicator which is directly linked to specific activities and/or objectives e.g., aimed at increasing diversity, equality, etc. |

Sources: SPARTA GA objectives, Technopolis Group, 2021

*Table A2 Relevance of SPARTA KPI for the original objectives of the call*

| **Key WP ICT-03-2018 call objectives and their links to SPARTA objectives** | | **Examples of possible KPIs** | **Relevant SPARTA KPI** |
|---|---|---|---|
| Common research, development, and innovation in next generation industrial and civilian cybersecurity technologies (including dual use), applications and services; focus should be on horizontal cybersecurity technologies as well as on cybersecurity in critical sectors; | 1-4, 7 | Contribution of the action to the (increase in) the number of projects and funding volumes allocated to (1) horizontal cybersecurity technologies, (2) cybersecurity critical sectors, (3) next gen industrial, civilian, and dual-use technologies. | #4.x, #7.1, #7.2, #7.3 |
| Strengthening cybersecurity capacities across the EU and closing the cyber skills gap; | 1-4, 6, 7 | Contribution of the action to the (increase in) the number of projects and funding volumes allocated to European cyber skills competence gaps. | #4.x, #6.2, #7.1, #7.2, #7.3 |

| | | | |
|---|---|---|---|
| Supporting certification authorities with testing and validation labs equipped with state-of-the-art technologies and expertise. | 1, 3, 4 | Contribution of the action to the (increase in) the number of competent certification authorities with testing and validation labs equipped with state-of-the-art technologies and expertise, and volumes of their activities. | #4.3, #5.x |
| Bring together cybersecurity R&D&I centres in Europe to create synergies and scale up existing competences and demonstrated strengths to the European level. Take into consideration relevant active digital ecosystems and public-private cooperation models and focus on solving technological and industrial challenges. Collectively develop and implement a Cybersecurity Roadmap. The results of the work done by the cPPP on cybersecurity, notably its Strategic Research and Innovation Agenda, will serve as a starting point. Consideration should also be given to the relevant work of ENISA, Europol and other EU agencies and bodies. | 1-7 | Percentage (or increase in) coverage of cybersecurity R&D&I centres in Europe in the relevant networks.<br>Increase in competences of cybersecurity R&D&I centres in Europe (requires a separate model for assessing the competence level), how many, where and how much. | #2.2, #2.3, #3.2, #4.x, #5.x, #6.x, #7.x |
| Set up a functional network of centres of expertise with a coordinating "competence centre". Work includes the assessment of various organisational and legal solutions for the Cybersecurity Competence Network, taking into account various criteria, including the EU mechanisms and rules, national and regional funding structures, as well as those offered by industry. Based on the above work, a governance structure should be proposed and will be implemented, tested and validated in the demonstration cases involving all partners in the network to showcase (in a measurable manner) its performance and optimise the suggested governance structure. | 1, 3 | Number of alternative governance models and arrangements tested and analysed.<br>Percentage coverage of all relevant legal issues related to governance of a multinational cybersecurity research network. | #1.3, #3.2 |
| Demonstrate the effectiveness of their selected governance structure by providing collaborative solutions to enhance cybersecurity capacities of the network and develop cyber skills. | 1, 5, 6 | Number of attendees in trainings based on jointly developed curricula. Satisfaction of trainees and their employers.<br>Increase in organisational competences (requires a separate model or tool for assessing competence level), how many, where and how much. | #5.2, #5.3, #5.4, #6.x |
| Ensure outreach, to raise knowledge and awareness of cybersecurity issues among a wider circle of professionals, where possible in cooperation with EU and national efforts, and to spread the developed expertise. | 6 | Contribution of the action (and/or collaborative action) to the increase in cybersecurity awareness and/or knowledge among people and organisations (requires a separate model or tool for assessing awareness and/or knowledge level), how many, where and how much. | #3.x, #6.x |
| Include industrial partners and their cybersecurity research collaborators to create synergies and: (a) collaboratively identify and analyse scalable cybersecurity industrial challenges in the selected sectors and (b) demonstrate their ability to collaborate in developing appropriate solutions to solve critical challenges through (not less than four) research and innovation demonstration cases. | 1, 3, 4 | Participation of different types of actors in defining the roadmap, and the number of their contributions.<br>Numbers and funding volumes of new joint project launched as the result of the roadmap and related action. Number of actors participating in the joint projects. | #2.x |

| | | | |
|---|---|---|---|
| These demonstration cases will constitute the core part of the work to be done within the project. They will be based on a specific research & development roadmap to tackle selected industrial challenges and will implement it covering a complete range of activities, from research & innovation through testing, experimentation, and validation to certification activities. | 7 | Number of commercially viable applications in (1) testing, (2) experimentation and piloting, (3) validation, (4) launched to the market.<br>Number of licencing agreements and start-ups originating from the activities. | #7.1, #7.1, #7.3 |
| Proposals shall foresee resources for clustering activities with other projects funded under this topic. This task will contribute to the actual setup of the Cybersecurity Competence Network and a European Cybersecurity Research and Competence Centre at a later stage. | 1, 3 | Share of activities implemented in collaboration with other pilots.<br>Volumes of research using shared assets of the pilots. | #3.2 |

Sources: SPARTA GA objectives, Technopolis Group, 2021

# Appendix B Bibliography


COM/2018/630 final. Proposal for a regulation of the European Parliament and of the Council establishing the European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres Final regulation proposal. European Commission. https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM%3A2018%3A630%3AFIN

Cyber Competence Network. (n.d.). About. Retrieved from: https://cybercompetencenetwork.eu/about/

Cyber Security for Europe. (n.d.). Our Community. Retrieved from: https://cybersec4europe.eu/our-community/

DG Research and Innovation. (2017). Meta-Evaluation of Article 185 Initiatives: Report of the Expert Group. https://www.era-learn.eu/documents/a185_meta_evaluation_expert_group_report-1.pdf

DG Research and Innovation. (2017). Mid-term review of the contractual Public Private Partnerships (cPPPs) under Horizon 2020: Report of the Independent Expert Group https://op.europa.eu/en/publication-detail/-/publication/6de81abe-a71c-11e7-837e-01aa75ed71a1

European Commission. (2017). Special Eurobarometer 464a – Europeans' attitudes towards cyber security. https://digital-strategy.ec.europa.eu/en/library/special-eurobarometer-europeans-attitudes-towards-cyber-security

European Commission. (2019). SPARTA DoA ANNEX 1 (part A), SPARTA Project – Strategic programs for advanced research and technology in Europe

European Commission. (2019). SPARTA DoA ANNEX 1 (part B), SPARTA Project – Strategic programs for advanced research and technology in Europe

European Commission. (2017). SU-ICT-03-2018 call for proposal - Establishing and operating a pilot for a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research & Innovation Roadmap. https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/su-ict-03-2018

European Parliament. (2019). Briefing – The new European cybersecurity competence centre and network. https://www.europarl.europa.eu/thinktank/en/document.html?reference=EPRS_BRI(2019)635518

European Cybersecurity Industry Leaders. (2016). Recommendations on Cybersecurity for Europe. https://www.eusemiconductors.eu/esia/public-policy/competitiveness-innovation

European Cyber Security Organisation. (n.d.). About the cPPP. Retrieved from: https://ecs-org.eu/cppp

European Cyber Security Organisation. (n.d.). Mission & Objectives. Retrieved from: http://www.ecs-org.eu/about

PwC. (2016). The Global State of Information Security Survey 2016. https://www.pwc.ru/en/publications/gsiss-2016.html

SPARTA. (2020). D1.1 Bootstrapping a CCN pilot. European Commission. https://www.sparta.eu/deliverables/

SPARTA. (2020). D1.2 Lessons learned from internally assessing a CCN pilot. European Commission. https://www.sparta.eu/deliverables/

SPARTA. (due for publication in 2021). D1.3. Improving a CCN pilot. European Commission

SPARTA. (2020). D8.1 Initial results of the clustering, platforms, and ecosystem activities. European Commission. https://www.sparta.eu/deliverables/

SPARTA. (due for publication in 2021). D8.2 Intermediate results of the clustering, platforms, and ecosystem activities. European Commission

SPARTA. (due for publication in 2021). D12.4 Updated dissemination and communication plan and evaluation. European Commission.

technopolis group

www.technopolis-group.com

# TECHNICAL SPECIFICATION

LIEU-DATE : NOVEMBER 19, 2020 SIGNATURE :

/ :

ÉMETTEUR : Thibaud ANTIGNAC / :

# Assessment of governance for a European Cybersecurity Competence Network pilot

## 1. Presentation of the expected work

### 1.1 Brief description

This is a call for tenders for performing an assessment of the governance for SPARTA, a European Cybersecurity Competence Network. This assessment will be executed from early-February 2021 to late March 2021.

### 1.2 Context

#### 1.2.1 Organizations involved

The French Alternative Energies and Atomic Energy Commission (CEA) is a key player in research, development, and innovation. Drawing on the widely acknowledged expertise gained by its 16,000 staff spanned over 9 research centers with a budget of 4.1 billion Euros, CEA actively participates in more than 400 European collaborative projects with a large number of academic and industrial partners. Within the CEA Technological Research Division, the CEA List institute addresses the challenges coming from smart digital systems. CEA is the coordinator of SPARTA (EU H2020 grant 830892[1]) and the procurement organizer, with which the contract will be signed.

The Fraunhofer Institute for Systems and Innovation Research (ISI) is an institution of the Fraunhofer Society, the biggest organization for applied research and development in Germany. Fraunhofer ISI is a beneficiary partner of SPARTA, responsible for the overall governance assessment in SPARTA, and will be a key partner in the assessment performed as a result of the contract. In particular, the documents submitted by the bidders may be shared by CEA with Fraunhofer ISI, under the NDA of an already existing consortium agreement signed in the context of the execution of SPARTA.

#### 1.2.2 SPARTA pilot

The EC-funded project SPARTA is a pilot for exploring organizational, procedural and institutional prerequisites for a future European Cybersecurity Competence Network (CCN) in

[1] See: https://cordis.europa.eu/project/id/830892/fr

the context of the upcoming European Cybersecurity Competence Centre (ECCC)[2]. The SPARTA project has started in February 2019 and will run until February 2022.
SPARTA is structured into 14 "Programs" (denoting technical activities) and "Activities" (denoting horizontal/transversal activities) ranging from WP1 to WP14 with a variety of sub-tasks. The *research part* of the project is comprised of four pillars (technical programs, WP4-WP7) and six cross-cutting activities (WP2, WP3, WP8, WP9, WP10, WP11, WP12). WP1 is dedicated to all aspects of the *pilot governance*, while WP13 and WP14 are concerned with aspects of *project management*.
In its first year (Y1) SPARTA's governance was assessed internally and documented in two deliverables. D1.2[3] investigated the pilot's Network-level governance during the project's ramp-up phase. At that stage, few demonstrative artifacts had been produced yet, so the study mainly assessed the implementation of governance structures and processes and their potential for future effective pilot governance. In view of the objectives stated in the project's DoW and external expectations and requirements, a set of assessment aspects, criteria and indicators were developed and validated. The majority of them remains to be applicable. A second internal assessment, D2.2[4], concerned a single Activity, namely of WP2, which is dedicated to ethical, legal and social aspects arising in the context of SPARTA's activities. D2.2 was guided by an industry-grade framework (COBIT). The study will be repeated in the second year (Y2) of the project. It could serve as a template for assessing the governance of other Programs and Activities but should not be considered as a strong constraint.
In accordance with SPARTA's Description of Work (DoW), the Y2-assessment will be carried out by an organization that is not a member of the consortium. Elements of this assessment will be used to become parts of SPARTA's Y2 deliverable D1.4 (*Lessons learned from externally assessing a CCN pilot*), which is planned to be due on April 30, 2021. The results of the Y2-assessment should thus be made available by March 31, 2021.

## 1.3 High Level Objectives

The external assessment under tender should support SPARTA's governance in offering an independent perspective on its structures, processes and activities, both in the context of the current pilot and as experimental template for a future, real-world CCN and ECCC. Possible areas for adjustment and improvement should be determined in the context of D1.4.
The external assessment should evaluate governance at (1) Network-level and (2) Program- and Activity-level, that is, covering SPARTA's technical and non-technical work packages during Y2 (Feb 2020-Jan 2021). Both types of governance should be assessed in view of their alignment with:

- The original Call for Proposals (CfP);
- Goals and objectives stated in SPARTA's Description of Work (DoW);
- The provisional legal and institutional framework envisaged by the European Institutions;
- The relevance for a future, institutionalized CCN and ECCC.

The external assessment should employ a framework of clearly defined methods, criteria, and indicators allowing to determine the degree of effectiveness of SPARTA's governance to advance:

- The technical and non-technical goals and objectives stated in the foundational documents (Call for Project Proposal, SPARTA Description of Work);
- The adoption of novel technical and non-technical challenges that may have arisen during the lifetime of the project so far (if applicable)[5].

## 1.4 Work perimeter

The following aspects are **in scope**:

[2] See: https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/su-ict-03-2018
[3] See https://www.sparta.eu/assets/deliverables/SPARTA-D1.2-Lessons-learned-from-internally-assessing-a-CCN-pilot-PU-M12.pdf
[4] See https://www.sparta.eu/assets/deliverables/SPARTA-D2.2-First-internal-ELSA-audit-and-supervision-report-PU-M12.pdf
[5] Novel challenges may arise e.g. from a changing research-political context, including those of expectations from EU institutions, from recent technical or societal development and change, or from co-operative activities with other CCN pilots.

- (1a) *Governance structure, processes and activities* for the SPARTA pilot carried out in the context of Activity WP1 during Y2, including (1b) the roles and integrative effects of the horizontal Activities WP2, WP3, WP8, WP9, WP10, WP11, and WP12.
- (2) *Governance structure, processes, and governance activities* for the SPARTA technical Programs carried out in the context of Programs WP4-WP7 during Y2.
- (3) *Degree of integration between and interactions across* technical Programs and horizontal Activities, tasks, technical and non-technical strands of work, and individual partners.
- (4a) *Adequacy, coverage, and continued relevance of indicators* used for the internal Y1 assessments D1.2 and D.2.2, (4b) selection and application of suitable indicators, metrics, and methods, (4c) revisiting and updating results and recommendations of D1.2 and D2.2.

The following aspects are **out of scope** for the external assessment:

- day-to-day technical and organizational project management (tracked and assessed by Activities WP13 and WP14);
- (2) operations and technical progress and execution of the R&D&I Programs WP4-WP7 (tracked and assessed by WP13);
- (3) operations and progress of the ELSA WP2 Activity (already covered by deliverable D2.4).

## 1.5 Stakeholders

The internal stakeholders comprise of the 44 beneficiary partner organizations of the SPARTA project consortium. The external assessment will mainly interact with representatives of those members who participate in SPARTA's governance Activity (WP1), in functions e.g. as:

- representatives of the SPARTA executive board,
- representatives of the SPARTA strategic direction,
- leaders of Programs and Activities,
- members of dedicated task forces, sub-boards committees.

SPARTA pilot governance also involves interactions with external stakeholders, e.g

- European Institutions and agencies,
- National Institutions and agencies,
- Professional Bodies,
- Institutions and organizations who joined the SPARTA associates program,
- Other ECCC/CCN pilots.

Interactions between SPARTA's pilot governance and the external stakeholders tend to be of confidential nature and are not subject to the external assessment.

# 2. Documentation and material available

The assessment of the SPARTA's governance should be based on empirical interviews or questionnaires with Activity and Program leaders, on pilot governance representatives, on public documentation, and on deliverables that have been made available by the project [6]. The existing deliverables formally accepted by the Financing Authority can be downloaded from the SPARTA website[7].

Pending public deliverables for the Y2 of the project will be made available as pre-versions as soon as possible. Other than this, the following external documents set the context for SPARTA's activities:

- Call for proposals: EC call for proposals (2017): Establishing and operating a pilot for a Cybersecurity Competence Network to develop and implement a common Cybersecurity Research & Innovation Roadmap. Oct 27, 2017[8];
- Scoping of political context and institutional framework: Proposal for a REGULATION OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL establishing the

[6] If information from other internal or external stakeholders is required, it may be solicited with the endorsement of the SPARTA coordinator and in co-operation with Fraunhofer ISI as the responsible editor for the overall assessment document D1.4.

[7] See https://www.sparta.eu/assets/deliverables/

[8] See https://ec.europa.eu/info/funding-tenders/opportunities/portal/screen/opportunities/topic-details/su-ict-03-2018

European Cybersecurity Industrial, Technology and Research Competence Centre and the Network of National Coordination Centres A contribution from the European Commission to the Leaders' meeting in Salzburg on 19-20 September 2018[9].

# 3. Work objective

## 3.1 Tasks

**Task 1: Development of approach, methods, and instruments**
Understand SPARTA objectives and activities; get familiar with criteria and methods of the SPARTA-internal assessments from Y1 and Y2. Adjust, extend or determine criteria for assessing (a) Network- and (b) Program- and Activity-level governance and develop an integrated approach in coordination with SPARTA's task T1.4. Document scope, indicators, methods, metrics. Develop structure of interviews and or questionnaires for (a) and (b). Develop a plan and timeline collecting the empirical data.
**Task 2: Data collection, categorization, and evaluation for Network-level pilot governance**
Develop, schedule, and execute a survey for assessing the *Network-level governance* by means of interviews, questionnaires or similar methods. Analyze, evaluate, present and document the results. Map results to corresponding indicators and data points from previous deliverables and reports where possible.
**Task 3: Data collection, categorization, and evaluation for Program- and Activity-level pilot governance**
Develop, schedule, and execute a survey for assessing the *Program- and Activity-level governance* by means of interviews, questionnaires or similar methods. Analyze, evaluate, present and document the results. Map results to corresponding indicators and data points from previous deliverables and reports where possible.
**Task 4: Integration of the assessments and presentation of results for the pilot governance**
Present and discuss the findings about SPARTA's Program- and Activity-level governance in view of their implications for SPARTA's Network-level governance. Present and discuss SPARTA's Network-level governance in view of stated goals, adequacy of its aspects as a template for a future CCN and ECCC, and its implications for interactions with external stakeholders. The integrated assessment method and the presentation format should be re-usable for a similar exercise of assessing SPATA's governance at the end of the project's lifetime. This will also include preliminary elements related to policy recommendations.

## 3.2 Methods

For reasons of continuity between the Network-level governance assessments of Y1 and Y2, the external assessment should consider adopting a subset of aspects, indicators and methods that were employed for the past internal assessment D1.2. This subset may have to be adjusted and extended accordingly. This applies in equal terms to the assessment at Program- and Activity-level, where D2.2 could provide a template. Taking guidance semi-formal, industry-grade assessment method would increase the chances of adopting elements of the assessment methodology for the Y3 evaluation and for a real-world CCN scenario.

# 4. Detailed work description

## 4.1 Task 1: Development of approach, methods, and instruments

### 4.1.1 Context

The SPARTA pilot has made substantial progress since its first internal governance assessment in January 2020. Consequently, the focus and criteria for the Y1 assessments have to be re-visited and adjusted. Complementary to evaluating the *implementation level* and the *potentials* of Network-level pilot governance of Y1, the Y2 assessment regards practical feasibility, efficiency, and impact of governance structures, processes and activities.

[9] See https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52018PC0630

### 4.1.2 Objectives

The assessment should focus on the practical efficiency of pilot governance, regarding (a) internal steering processes and (b) interactions and interfaces with external stakeholders. It should determine indicators for evaluating the relevance and appropriateness of the pilot governance in view of a future, real-world scenario. The methodological approach selected should partially be based on empirical data. Interview structures and / or questionnaires have to be designed accordingly. The work must also yield a plan and schedule for collecting and evaluating the required data.

### 4.1.3 Work to be performed

- Get acquainted with current SPARTA project and pilot context with focus on governance aspects. Base documents are the Call for Proposals, the corresponding EU documents on ECCC / CCNs, goals and objectives from Description of Work.
- Get acquainted with the methodological approaches used in SPARTA's Y1 deliverables D1.2, D2.2. Revisit and adjust criteria and indicators developed therein; determine additional criteria and indicators if so required.
- Revisit, adopt and/or adjust the methodological approaches used in D1.2, D2.2. Define the methods used for the assessment. Determine and validate the set of empirical data required for assessing SPARTA's pilot governance at both Network- and Program- and Activity-level.
- Develop questionnaires and / or structured interviews according to the criteria and in indicators. Develop a data collection plan (stakeholders, timeline). Schedule interviews with SPARTA WP1 Activity, informing them about questionnaire deadlines. **Note:** the sample size (number of individuals to be questioned and / or interviewed) ranges between 15 and 25.

### 4.1.4 Level of detail expected

Assessment of governance at Program- and Activity-level should distinguish concerns that mainly concern Network-level *pilot governance* from those primarily related to *operational project management* such as timeliness of ongoing research, resourcing, finance, and conformance to the DoW. The same applies e.g. to levels of achievement for specific technical and non-technical objectives, which are already tracked by operational management. (see section 1.4.)

## Task 2: Data collection, categorization, and evaluation for Network-level pilot governance

### 4.2.1 Context

SPARTA's Network-level governance comprises the technical lead of the pilot, the executive board and strategic direction, operational project management, and various thematic task forces. Its acting members are typically Program and Activity leaders who represent the pilot's different activities. Network-level governance has (a) to ensure that the results of the Programs and Activities are in accordance with the goals of the pilot and assumed objectives of a future European CCN. It also has (b) to initiate and maintain interactions with variety of relevant stakeholder groups (political administration, national and international agencies, professional bodies, commercial organizations). Last, it has (c) to monitor and to react to relevant shifts in the research-political and technical landscape of cybersecurity.

### 4.2.2 Objectives

Assessing the effectiveness and agility of Network-level governance with regards to the objectives (a), (b), (c) listed above.

### 4.2.3 Work to be performed

- Collect information from members of the Network-level pilot management group via interviews and questionnaires. Transcribe the interviews. Mark the sections constituting data points (if applicable).
- Process and analyze the empirical data in accordance with the method developed in Task 1 (aspects, indicators, metrics, etc.)
- Structure the results in such a way as to support an integrated analysis and presentation with results of Task 3.

### 4.2.4 Level of detail expected

SPARTA's Description of Work requires a lean assessment that does not impose undue workload on the participants. The duration interviews should not exceed 60 minutes; questionnaires should not exceed 25 questions.

## Task 3 Data collection, categorization, and evaluation for Program- and Activity-level pilot governance

### 4.3.1 Context

The design of SPARTA's Programs and Activities models future tasks and processes of a real-world European CCN. Consequently, the technical work packages (WP4, 5, 6, and 7), also called “Programs”, are treated as semi-autonomous projects in their own right. Their leaders have been given reign to optimize Program- and Activity-level governance according to their specific needs and requirements, that is (a) to achieve their technical objectives and (b) to advance the goals of the pilot as a whole. Aspect (a) is covered at Program- and Activity-level and by SPARTA's operational management, already, so the focus of the assessment is aspect (b).

Work packages 2, 3, 8, 9, 10, 11, and 12, also called “Activities”, are of transversal nature. They address intersections between Network-level goals of the CCN pilot and the technical activities, and operate at interfaces with particular external stakeholders. These Activities are to be assessed (a) regarding their interactions with the Programs, (b) their potential and actual impact on parts of the external cybersecurity ecosystem, and (c) their supportive function for Network-level pilot governance.

### 4.3.2 Objectives

Assessing the effectiveness and agility of Network-level governance with regards to the requirements (b) listed above (for the Programs on one hand, and for the Activities on the other hand).

### 4.3.3 Work to be performed

- Collect information from Program and Activity leaders via interviews and questionnaires. Transcribe the interviews. Mark the sections that are to be used as data points (if applicable).
- Process and analyze the empirical data in accordance with the method developed in Task 1 (aspects, indicators, metrics, etc.)
- Structure the results in such a way as to support an integrated analysis and presentation with results of Task 2

### 4.3.4 Level of detail expected

See 4.2.4. In addition:

- Note that WP2 is assessed internally on an ongoing basis. The internal assessment will be carried out when external assessment also takes place, and both activities should be coordinated in regard to scheduling and coverage.
- The internal Activity WP2 assessment is guided by the assessment framework COBIT (see D2.2). Its approach should be considered for the external assessment of other Programs and Activities.

## 4.4 Task 4 Integration of the assessments and presentation of results for the pilot governance

### 4.4.1 Context

Network- and Program- and Activity-level governance are mutually dependent. The methods applied for Task 2 and Task 3 should be complementary. Methods and presentation format should lend themselves to future applicability for a full-fledge CCN.

### 4.4.2 Objectives

Report comprising of the results of Tasks 1, 2, 3, an integrated analysis and presentation.

### 4.4.3 Work to be performed

- Combine results from Tasks 2 and 3, present assessment aspects in view of their current relevance, level of achievements, and potential for improvement and adjustment through propositions
- Present the state of pilot governance in an integrated way, using quantified or quantized representation where possible.

- Highlight aspects that may require adjustment, and suggest corrective actions.
- Propose accompanying elements forming a basis for policy suggestions enabling to leverage the above propositions.

#### 4.4.4 Level of detail expected

The expected level of detail corresponds to that of Task 2 and Task 3. The integrated presentation should be detailed enough to support adjustment decisions. Suggestions for adjustments should be qualified in regard of the responsibilities of (1) Network-level governance, (2) Program- and Activity-level governance, or (3) operational management.

# 5. Deliverables and Milestones

## 5.1 Schedule

| *Deliverable submission* | *Execution timeline* |
|---|---|
| Phase 1: Development of approach, methods and instruments<br>Task 1 | |
| D1.1 First Meeting about methodological approaches<br>D1.2 Methodological approach defined and documented | D1.1 by the end of T0 + 2 weeks<br><br>**D1.2 by [to be proposed by bidder]**<br><br>Milestone 1 |
| Phase 2: Data collection and categorization for pilot governance<br>Task 2 and 3 | |
| D2 Questionnaires, interview structures, and transcripts | **D2 by [to be proposed by bidder]**<br><br>Milestone 2 |
| Phase 3: Data evaluation for pilot governance<br>Task 2 and 3 | |
| D3 Evaluation of SPARTA's Network-, Program- and Activity-level governance | **D3 by [to be proposed by bidder]**<br><br>Milestone 3 |
| Phase 4: Integration of the assessments and presentation of results for the pilot governance<br>Task 4 | |
| D4.1 Second Meeting about assessment integration<br>D4.2 Integrated assessment document | D4.1 by March 17, 2021<br><br>D4.2 by March 31, 2021<br>Milestone 4 |

T0 is estimated to be early February; the precise date might vary depending on when the contract is actually signed.

## 5.1 Deliverable format

- D1.1 Slides, discussion minutes, and intermediate state of D1.2
- D1.2 Report and updated slides from D1.1
- D2 Report and transcripts
- D3 Report
- D4.1 Slides, discussion minutes, and intermediate state of D4.2
- D4.2 Report and updated slides from D4.1

# 6 Execution

### 6.1 Communication

By default, communication will be based on email, telephone and teleconferencing. Each milestone will be accompanied by a teleconference or meeting between the contracting entity and the contractor. Interviews will be carried out by teleconference unless extraordinary circumstances suggest personal encounters.

### 6.2 Meetings
Conditions allowing, physical meetings should take place (a) at the beginning of the work period (mid-February 2021, D1.1) and (b) for discussing the pre-version of the final report one week prior to its submission (mid-March 2021, D4.1). These meetings will be organized as teleconferences if conditions do not allow for physical meetings.

### 6.3 Milestones
See section 5: completion of each phase corresponds to a dedicated milestone.

## 6.4 Control

### 6.4.1 Monitoring
Progress is monitored by means of bi-weekly telephone conferences and by dedicated meetings / teleconferences for each milestone.

### 6.4.2 Acceptance of Deliverable
A preliminary version of each deliverable should be submitted to CEA, as the contracting entity, at least 7 days before its final version is due.

### 6.4.3 Location
The work is location-independent.

## 6.5 Contacts
Thibaud Antignac thibaud.antignac@cea.fr +33 1 69 08 07 42

# 7. Evaluation

## 7.1 Tender
The tender should describe the methodology envisaged to address the tasks at an appropriate level of detail. The tender must include a description of the organization, roles and responsibilities, skills, experience in the field of staff, short biographies of example of staff involved, and a price calculation.

## 7.2 Proof of Eligibility
The bidder must provide the following documents to demonstrate eligibility:

1. Company profile
2. Information on turnover for the past three financial years.
3. Self-declaration on the proper payment of taxes, duties and contributions to statutory social security.
4. Self-declaration that no insolvency proceedings have been opened, are pending, or have been rejected due to lack of funds, and that the company is not in liquidation.
5. Self-declaration that no serious misconduct has been committed that questions the reliability of the applicant.
6. Self-declaration that the bidder is not a partner or associated to any of the four pilots (SPARTA (EU H2020 830892 grant), CONCORDIA (EU H2020 830927 grant), ECHO (EU H2020 830943 grant), CyberSec4Europe (EU H2020 830929 grant)).
7. Project references from the past 3 years to demonstrate the following eligibility criteria:
   - Practical experience in assessing or auditing national or international research projects.
   - Practical experience in co-operating with scientific research projects.
   - Experience in analyzing and assessing institutional configurations and authorities
   - provide for each reference at least (1) Customer name and contact details, (2) a description of the work carried out, (3) the effort (in person-weeks), (4) the means of implementation means and (5) a description of the planning methods employed
8. Demonstration of the qualifications of the personnel involved in the assessment:
   - For tasks listed under (6), at least 3 years of practical experience in assessments in different fields

- Familiarity with the cybersecurity ecosystem at national or European level (Bonus)
- Familiarity with industry-grade assessment frameworks (Bonus)
- Evidence: examples of representative CVs

## 7.2 Calculation

The bidder must submit a calculation of the price for the service offered. The following points must be taken into account:

- The price calculation must be structured by task, spelling out the effort in person weeks.
- Costs for subcontracts that exclude VAT may only be calculated with their net amount if the bidder calculates with VAT and would be entitled to corresponding tax deductions.
- For bidding consortia, the respective assignment of the service, the responsibilities and the costs must be recognizable. Bidder consortia must provide their temporary business grouping contract
- In order to be accepted, the bid must include the final price of the offer (except travel costs);
- Travel costs will be arranged separately and refunded on notification of paid invoices. Travel costs will be limited to 120€ per night (including breakfast), 17.50€ for lunch, 17.50€ for dinner, economy fares for flights and 1st class fares for trains. Travel costs will be capped to a maximum of 5000€ (excluding VAT).

## 7.4 Attachments to the offer

The documents listed below must be submitted in full with the offer. Incomplete documents may lead to exclusion from the selection procedure.

(1) Calculation of Price
(2) Proof of Eligibility documents

# 9. Data Protection

The contractor must not disclose information about interviewees and respondents to questionnaires that may allow personal identification. All raw and processed data for the assessment must reside on storage facilities inside the European Union.

Telephone interviews and surveys in writing must not be outsourced to third parties. Audio data from oral interviews must not be processed by neither automated nor non-automated transcription services residing outside the European Union. Data from interviews and questionnaires must be encrypted prior to transfers across electronic networks resp. storing for archiving. Assessment-related data and archives must not be retained beyond the lifetime of SPARTA (February 2022), except documents related to an audit ordered or conducted by the European Commission.